IAM 2.1 User Manual

September, 2010

Table of Contents

Table of Contents **1**
Announcement **8**
Preface **9**
About This Manual 9
Document Conventions 10
Graphic Interface Conventions *10*
Symbol Conventions *11*
Technical Support 11
Acknowledgements 11
Chapter 1 IAM Installation **12**
1.1. Environment Requirement 12
1.2. Power 12
1.3. Product Appearance 12
1.4. Configuration and Management 13
1.5. Wiring Method of Standalone 13
1.6. Wiring Method of Redundant System 15
Chapter 2 Console **17**
2.1. Web UI Login 17
2.2. IAM Gateway Configuration 18
Chapter 3 System Status **19**
3.1. Running Status 19
3.2. Security Status 20
3.3. License 21
3.4. Gateway Mode 22
3.4.1. Route Mode *22*
3.4.2. Bridge Mode *24*
3.4.2.1. Bridge Mode: Multiple-Interface 25
3.4.2.2. Bridge Mode: Multi-Bridge 28
3.4.3. Bypass Mode *31*
3.4.4. Single-Arm Mode *34*
3.5. Network Interface 37
3.6. Multi-Node Sync 38
3.7. Date/Time 40
3.8. Administrators 40
3.9. WEBUI 43

3.10. Backup/Restore 44
3.11. Reboot 45
3.12. Maintenance 45
3.13. Auto Update 46
3.14. Route 47
3.14.1. Policy Routing *47*
3.14.2. Static Routing *50*
3.15. Generate Certificate 53
3.16. High Availability 53
Chapter 4 Object 56
4.1. Application Ident Rule 56
4.2. Intelligent Ident Rule 59
4.3. Service 61
4.4. IP Group 62
4.5. Schedule 64
4.6. URL Group 65
4.7. White List Group 68
4.8. Keyword Group 69
4.9. File Type Group 70
4.10. Ingress Rule 71
4.11. SSL Certificate 80
Chapter 5 Firewall 82
5.1. Firewall Rule 82
5.1.1. LAN <-> DMZ *82*
5.1.2. DMZ <-> WAN *84*
5.1.3. WAN<->LAN *84*
5.1.4. VPN <-> WAN *85*
5.1.5. VPN<->LAN *86*
5.1.6. LAN<->LAN *87*
5.1.7. DMZ <-> DMZ *88*
5.2. NAT Rules 88
5.2.1. SNAT *89*
5.2.2. DNAT *90*
5.3. Anti-DoS 92
5.4. ARP Protection 95
Chapter 6 WAN Optimization 97
6.1. Optimization Status 97

6.1.1. System Status *98*
6.1.2. Optimization Status *98*
6.1.3. Cache Hit *100*
6.2. Proxy Options 101
6.2.1. System Settings *102*
6.2.1.1. Basic Settings 104
6.2.1.2. Advanced Settings 105
Chapter 7 IAM 107
7.1. Access Control Policy 107
7.1.1. Add Access Control Policy *109*
7.1.2. Edit Access Control Policy *111*
7.1.2.1. Access Control 112
7.1.2.1.1. Application Control 113
7.1.2.1.2. Service Control 114
7.1.2.1.3. Proxy Control 116
7.1.2.2. Web Filter 117
7.1.2.2.1. HTTP URL Filter 117
7.1.2.2.2. HTTPS URL Filter 120
7.1.2.2.3. Keyword Filter 122
7.1.2.2.4. File Type Filter 123
7.1.2.2.5. ActiveX Filter 126
7.1.2.2.6. Script Filter 130
7.1.2.3. Email Filter 131
7.1.2.3.1. Send/Receive Mail 131
7.1.2.3.2. Delayed Email Audit 132
7.1.2.4. SSL Management 134
7.1.2.4.1. SSL Control 134
7.1.2.4.2. SSL Content Ident 135
7.1.2.5. Application Audit 137
7.1.2.5.1. Audit Option 137
7.1.2.5.2. Outgoing File Alarm 140
7.1.2.6. Flow/Time Statistics 144
7.1.2.6.1. Flow/Time Statistics 144
7.1.2.6.2. Online Duration Control 145
7.1.2.6.3. Session Control 145
7.1.2.7. Ingress System 146
7.1.2.8. Risk Ident 147

7.1.2.9. Reminder 149
7.1.2.9.1. Time Reminder 149
7.1.2.9.2. Flow Reminder 150
7.1.2.9.3. Bulletin Page 151
7.2. Authentication Options 153
7.2.1. New User Authentication *153*
7.2.2. SSO Settings *156*
7.2.2.1. Active Directory SSO 157
7.2.2.1.1. Install Component Mode 158
7.2.2.1.2. AD Group Policy Mode 158
7.2.2.1.3. Configure Logon Script Program 159
7.2.2.1.4. Configure Logoff Script Program 163
7.2.2.2. POP3 SSO 166
7.2.2.2.1. POP3 Authentication 166
7.2.2.2.2. Network Environment 167
7.2.2.2.3. Configuration 167
7.2.2.3. WEB SSO 168
7.2.2.4. Proxy SSO 170
7.2.2.4.1. Proxy Authentication 170
7.2.2.4.2. Network Environment 170
7.2.2.4.3. Configuration 170
7.2.2.5. Listening Mirror Port 171
7.2.2.6. Only Allow SSO 171
7.2.3. Page Display After Authentication *172*
7.2.4. Authentication Conflict Settings *173*
7.2.5. SNMP Option *174*
7.2.6. Other Authentication Options *175*
7.3. Authentication Server 177
7.3.1. LDAP *178*
7.3.2. RADIUS *179*
7.3.3. POP3 ..... *180*
7.4. Organization Structure 180
7.4.1. Search *182*
7.4.2. Add Subgroup *183*
7.4.3. Edit Subgroup *185*
7.4.4. Edit User *190*
7.4.5. Edit User *192*

7.4.5.1. Binding IP/MAC 193
7.4.5.1.1. Bind IP 193
7.4.5.1.2. Bind MAC 194
7.4.5.1.3. Bind Both IP and MAC 196
7.4.5.1.4. No Binding 197
7.4.5.2. Group 197
7.4.5.3. Authentication Method 198
7.4.5.4. Expiry Date 200
7.4.5.5. Enable This User 201
7.4.5.6. Access Control Policy 203
7.5. User Import 204
7.6. LDAP Sync 206
7.6.1. Sync by LDAP Organization Structure 207
7.6.2. Sync by LDAP Security Group 209
7.6.3. View Sync Report 210
7.7. Online User 211
Chapter 8 Bandwidth Management 214
8.1. Bandwidth Status 214
8.1.1. Bandwidth Channel 215
8.1.2. Exclusion Policy 216
8.2. Bandwidth Settings 217
8.2.1. Bandwidth Channel 217
8.2.1.1. Add Bandwidth Channel 218
8.2.1.2. Add Child Bandwidth Channel 223
8.2.1.3. Select and Edit Bandwidth Channel 224
8.2.2. Exclusion Policy 226
8.3. Line Bandwidth 227
8.4. Virtual Line 227
Chapter 9 Delayed Email Audit 232
9.1. Email Audit Policy 232
9.2. Audited Email 233
9.3. Unaudited Email 233
Chapter 10 Internet Access Audit 234
10.1. Realtime Logs 234
10.1.1. Flow Ranking 235
10.1.2. Connection Ranking 237
10.1.3. Connection Monitoring 238

10.1.4. Behavior Monitoring *238*
10.2. Audit Log Maintenance 239
10.3. Data Center Settings 239
10.4. Enter Data Center 242
Chapter 11 Logs/Troubleshooting 244
11.1. System Logs 244
11.2. Policy Troubleshooting 246
11.3. Packet Capture 249
Chapter 12 Advanced 253
12.1. Alarm 253
12.2. Proxy Server 254
12.3. Web Tracking 255
12.4. Excluded IP/Domain 257
12.5. Page Customization 258
Chapter 13 Security 260
13.1. Gateway Antivirus 260
13.2. IPS 262
13.2.1. IPS Options *262*
13.2.2. IPS Rules *264*
13.3. VPN Settings 265
13.3.1. VPN Status *265*
13.3.2. Basic Settings *266*
13.3.3. User Management *269*
13.3.4. Connection Management *273*
13.3.5. Virtual IP Pool *276*
13.3.6. Multiline Settings *278*
13.3.7. Multiline Routing Policy *280*
13.3.8. Local Subnet List *284*
13.3.9. Tunnel Route *285*
13.3.10. IPSec Connection *289*
13.3.10.1. Device List 289
13.3.10.2. Security Option 291
13.3.10.3. Outbound Policy 293
13.3.10.4. Inbound Policy 294
13.3.11. Common Settings *296*
13.3.11.1. Schedule 296
13.3.11.2. Algorithm List 298

13.3.12. Advanced *298*
13.3.12.1. LAN Service 298
13.3.12.2. VPN Interface 302
13.3.12.3. LDAP Server 303
13.3.12.4. Radius Server 304
13.3.13. Generate Certificate *305*
Chapter 14 DHCP 306
14.1. DHCP Status 306
14.2. DHCP Settings 306
Chapter 15 Wizard 309
Appendix A: Gateway Client-Updater 310
Appendix B: Acronyms And Abbreviations 317

Announcement

Copyright © 2010 SANGFOR Technology Co., Ltd. All rights reserved.

No part of the contents of this document shall be extracted, reproduced or transmitted in any form or by any means without prior written permission of SANGFOR.

SANGFOR, SANGFOR Technology and the SANGFOR logo are the trademarks or registered trademarks of SANGFOR Technology Co., Ltd. All other trademarks used or mentioned herein belong to their respective owners.

This manual shall only be used as usage guide, and no statement, information, or suggestion in it shall be considered as implied or express warranty of any kind, unless otherwise stated. This manual is subject to change without notice. To obtain the latest version of this manual, please contact the Customer Service of SANGFOR Technology Co., Ltd.

Preface

About This Manual

The IAM2.1 User Manual includes the following chapters:

Chapter	Describe…
Chapter 1 IAM Installation	The product appearance, function features and performance parameters of IAM gateway device, and wiring and cautions before installation.
Chapter 2 Console	How to use the console and the general operation on the console.
Chapter 3 System Status	How to configure the device-related options, including status displays, license, gateway mode, network interface, multi-node synchronization, WEBUI, system date and time, backup/restore, reboot, maintenance and update.
Chapter 4 Object	Some related objects of IAM gateway and configuration of each of them, including the internal application/intelligent identification rules, user-defined identification rules, URL group, IP group, service, time schedule, white list group, keyword group, file type group, ingress rule, and SSL certificate.
Chapter 5 Firewall	How to configure the firewall rules of the IAM gateway, as well as the SNAT (source network address translation) rule and DNAT (destination network address translation) rule.
Chapter 6 WAN Optimization	How to configure WAN optimization module to achieve WAN optimization (acceleration).
Chapter 7 IAM	How to configure the access control policies, authentication method, organization structure, etc., of the IAM gateway.
Chapter 8 Bandwidth Management	How to view the bandwidth related information, and configure the bandwidth channel policy as well as bandwidth rule for line and virtual line.
Chapter 9 Delayed Email Audit	How to configure the email audit policy for some specified emails.
Chapter 10 Internet Access Audit	The internet access audit information, including viewing the internet access statistics in real time, log maintenance and Data Center settings, etc.

Chapter 11 Logs/Troubleshooting	The function and use of the system logs, policy troubleshooting and packet capture module.
Chapter 12 Advanced	How to configure the system related settings, such as alarm, proxy server, web tracking and page customization.
Chapter 13 Security	How to configure some extension functions and security-related modules provided by the SANGFOR IAM gateway, such as gateway antivirus, intrusion prevention system (IPS), VPN settings, IPSec connection, and some other common and advanced settings.
Chapter 14 DHCP	The function, use and configuration the DHCP service.
Chapter 15 Wizard	Where the configuration starts from and how to configure the IAM gateway step by step.

Document Conventions

Graphic Interface Conventions

This manual uses the following typographical conventions for special terms and instructions:

Convention	Meaning	Example
boldface	Keywords or highlighted items	The user name and password are **Admin** by default.
italics	Directories, URLs	Enter the following address in the IE address bar: *http://10.254.254.254:1000*
[ ]	Page titles, names of parameters, menus, and submenus	Select [System] > [Web UI] to open the Web UI page, and then configure the [Webpage Timeout].
< >	Names of buttons or links on the web interface or key-press	Click <Update> to save the settings.
>	Multilevel menus and submenus	Go to [System] > [Network Interface] to configure the network interfaces.
“ ”	Prompts popped up	The browser may pop up the prompt "Install ActiveX control"

Symbol Conventions

This manual also adopts the following symbols to indicate the parts which need special attention to be paid during the operation:

Convention	Meaning	Description
	Caution	Indicates actions that could cause setting error, loss of data or damage to the device.
	Warning	Indicates actions that could cause injury to human body.
	Note	Indicates helpful suggestion or supplementary information.

Technical Support

For technical support, use the following methods:

- Go to our official website: *http://www.sangfor.com*
- Go to our technical support forum: *http://www.sangfor.com/cn/forum*
- Call 800-830-6430 (fixed-line phone) or 400-830-6430 (mobile or fixed-line phone)
- Email us at: *support@sangfor.com.cn*

Acknowledgements

Thanks for using our product and user manual. If you have any suggestion about our product or user manual, please provide feedback to us through phone or email. Your suggestion will be much appreciated.

Chapter 1 IAM Installation

This chapter mainly describes the appearance of SANGFOR IAM series hardware gateway device and the installation. After correct installation, you can configure and debug the system.

1.1. Environment Requirement

The SANGFOR IAM device requires the following working environment:

- Input voltage: 110V-230V
- Temperature: -10-50℃
- Humidity: 5%-90%

To ensure long-term and stable running of system, the power supply should be properly grounded, dustproof measures taken, working environment well ventilated and indoor temperature kept stable. This product conforms to the requirements on environment protection, and the placement, usage and discard of the product should comply with relevant national law and regulation.

1.2. Power

The SANGFOR IAM series device uses 110 ~ 230V alternating current (AC) as its power supply. Make sure it is well-grounded before being provided with power supply.

1.3. Product Appearance

SANGFOR IAM hardware gateway device

Above is a SANGFOR IAM hardware gateway device. The interfaces or indicators on the front panel from left to right are described respectively as follows:

CONSOLE Interface: Interface used for high-availability function (redundant system)

USB Interface: Standard USB port connecting to the peripheral device

LAN Interface: Network interface, to be defined as LAN interface

DMZ Interface: Network interface, to be defined as DMZ interface

WAN1 Interface:	Network interface, to be defined as WAN1, LAN, or DMZ interface
WAN2 Interface:	Network interface, to be defined as WAN2, LAN, or DMZ interface
POWER:	Power indicator of IAM gateway device
ALARM:	Alarm indicator of IAM gateway device (it keeps on for one minute while the device is starting up)

- Normally, the **ALARM** indicator keeps on lighting (in red) when the device is starting and goes out in about one or two minutes, indicating successful startup of the device. After startup, the **ALARM** indicator may flash, which means the device is writing logs; however, if the **ALARM** indicator stays lighted for a long time and does not go out, please shut down the device, and about 5 minutes later restart the device once again. If this situation remains after restart, please contact our Customer Service to confirm whether the device is damaged.
- The **CONSOLE** interface is only for debugging by technicians. The end users connect to the device via the network interfaces.

1.4. Configuration and Management

Before configuring the device, please prepare a computer and make sure the web browser (for example, Internet Explorer browser) of the computer can be used normally. Then connect the computer to the IAM gateway device (in a same local area network) and configure the IAM gateway on the computer over the established network.

1.5. Wiring Method of Standalone

Connect the power cable to the **Power** interface on the rear panel of the IAM gateway device and switch on the power supply. The **POWER** indicator (in green) and **ALARM** indicator (in red) on the front panel will be lighted. The **ALARM** indicator will go out one or two minutes later, indicating the device runs normally.

Follow the instructions below to wire the interfaces:

Use standard RJ-45 Ethernet cable to connect the LAN interface to the local area network and then configure the IAM gateway device.

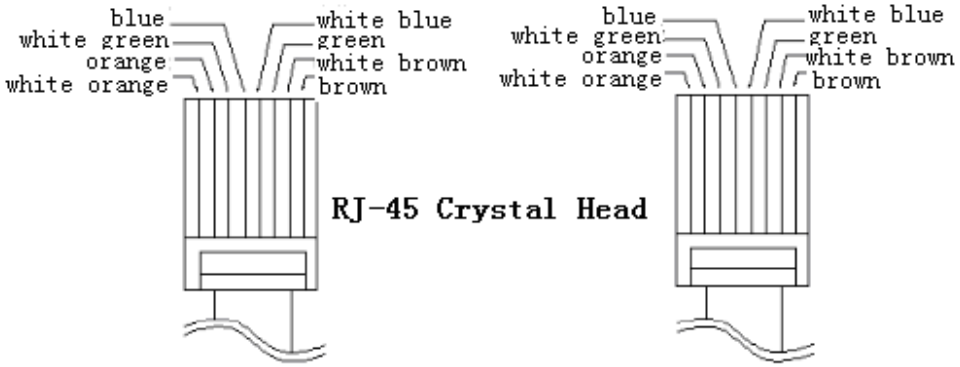
Use standard RJ-45 Ethernet cable to connect the WAN1 interface with the networking device,

such as router, optical fiber transceiver, ADSL Modem, etc.

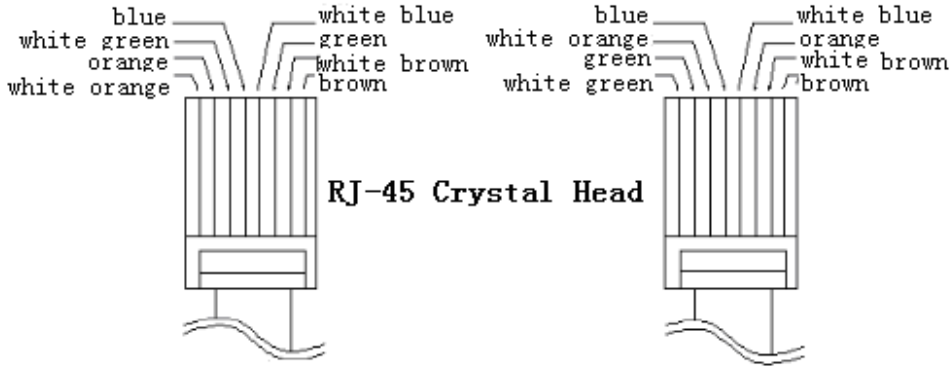
Use standard RJ-45 Ethernet cable to connect DMZ interface to the DMZ zone network. Generally, the Web server and Mail server providing services to wide area network (WAN) are placed at the DMZ zone. The IAM device provides secure protection for these servers.

- Multi-line function of the IAM gateway device allows multiple Internet lines to be connected in. You can connect the second Internet-access device to the **WAN2** interface.
- When IAM gateway device runs normally, the **POWER** indicator (in green) will keep on lighting, and the **WAN LINK** and **LAN LINK** indicators (in orange) will keep on lighting. The ACT indicators (in green) will flicker if there is data flow. The **ALARM** indicator will be lighted only for about one minute due to system loading when the device is starting and then go out, indicating successful startup of the device. If the **ALARM** indicator stays lighted during startup, please switch off the power and restart the device. If it still keeps on lighting and does not go out, please contact us.
- Please use straight-through cable to connect a WAN interface with the Modem, and crossover cable to connect a WAN interface with the router. Use straight-through cable to connect the LAN interface with the switch, and crossover cable to connect the LAN interface on the device with the network interface on the computer. If connections cannot be established while the corresponding indicator functions normally, please check whether the cables are correctly used for connections. The differences between straight-through cable and crossover cable are the wire sequences at both ends are different, as shown in the next figure.

1. Wire Sequence of Straight-through Cable



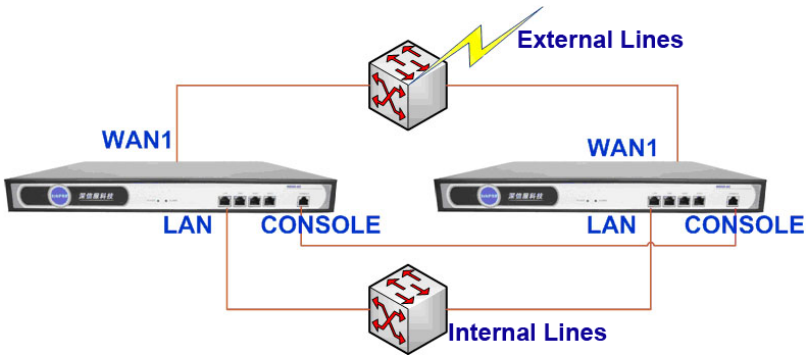
2. Wire Sequence of Crossover Cable



Wire Sequences of Straight-through Cable and Crossover Cable

1.6. Wiring Method of Redundant System

If two SANGFOR IAM gateway devices are deployed to work in high availability mode (HA), the wiring to the external network and internal network should be as shown in the following figure:



Use standard RJ-45 Ethernet cable to connect the WAN1 interfaces of the two IAM gateway devices to a same switch (if multi-line function is applied, the wiring is the same while the WAN interfaces of the two gateway devices should be ensured to be connected to a same external line);

then use a standard RJ-45 Ethernet cable to connect the IAM gateway device to other networking device such as router, fiber optical transceiver or ADSL Modem, etc.

Use the Console cable (among the accessories) to connect the serial ports of the two IAM gateway devices (through the **CONSOLE** interface).

Use RJ-45 Ethernet cable to connect the LAN interfaces of the two IAM gateway devices to a same switch, and then connect the switch to the local area network switch with standard RJ-45 wire, connecting it to the local area network (LAN).

Having completed wiring, you have to switch on the power of the two IAM gateway devices and then configure them. Device configuration of the HA system is the same with that of a single IAM gateway device; you need only configure one of the IAM gateway device, and the other IAM gateway device will synchronize and copy the settings automatically.

Chapter 2 Console

2.1. Web UI Login

IAM series gateway devices support secure HTTPS login, at standard HTTPS port. The login URL address is: https://10.251.251.251

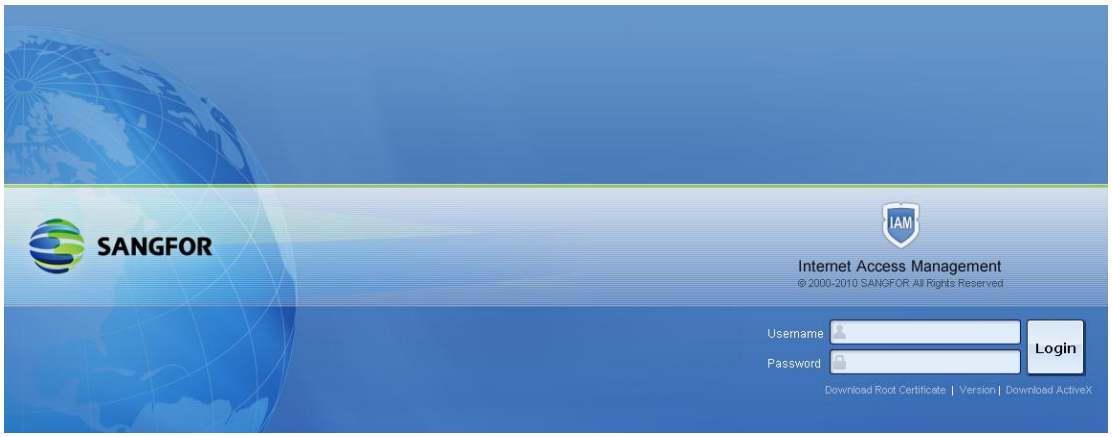
Log in through HTTPS to the WEB user interface (WEB UI) to manage the IAM gateway device, the potential risks caused by interceptions during transmission can be avoided.

Having connected all the wires, you can go on to configure the SANGFOR IAM gateway device through the WEB UI. Detailed procedures are as described in the following chapters.

Configure a valid IP address for the IAM gateway device. The IP address is of the 10.251.251.X network segment (such as 10.251.251.100). Then type the default login IP address and port of the IAM device in the IE browser, *https://10.251.251.251*, and the following pop-up warning dialog appears:

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Click the <Yes> button and the following login interface appears:



Before login, you may be required to install the pop-up ActiveX control. Click "This site might require the following ActiveX control: 'sangfor dcweb' from Sangfor Technology Co., Ltd'. Click here to install…" > "Install ActiveX Control…" and then follow the instructions to finish installation. If there is no prompt of installing the ActiveX control, click the <Download ActiveX> link to manually download the ActiveX control, and follow the instructions to finish installation.

Enter the user name and password; click the <Login> button or press <Enter> key to log in to the console of IAM gateway device. The user name and password are **Admin** by default.

If you want to view the version information, click the link <View Version>.

2.2. IAM Gateway Configuration

Logging in successfully, you will face the following function modules (left tree): [System], [Object], [Firewall], [IAM], [Bandwidth Management], [Delayed Email Audit], [Internet Access Audit], [Logs/Troubleshooting], [Security], [DHCP], [Wizard], etc.

In case there is a <OK> or <Finish> button on a configuration page, click it after altering/configuring the parameters to save or apply the settings. This will not be illustrated again in the subsequent parts in this user manual.

If you are to switch network interface (LAN interface and WAN-type interface) on the [Network Interface] page, the network connection will be interrupted and system requires rebooting the IAM system and re-login.

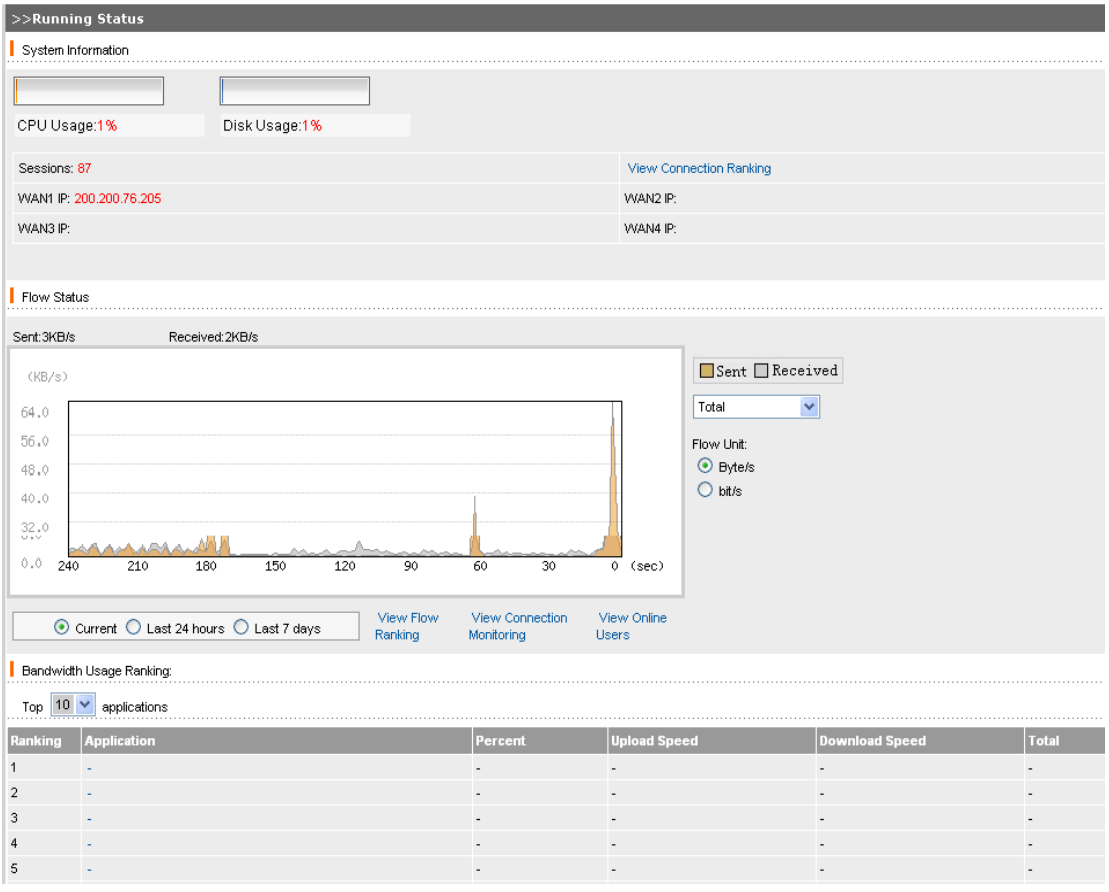
All the configuration pages have a <Help> link at the upper right corner. If help is wanted, click it to view the brief description of the item.

Chapter 3 System Status

[System] covers the running status of the IAM gateway device. Detailed sections are [Running Status], [Security Status], [License], [Gateway Mode], [Network Interface], [Date/Time], [Administrators], [WEB UI], [Backup/Restore], [Reboot], [Auto Update], [Route], [Generate Certificate], etc.

3.1. Running Status

[Running Status] provides the real-time status of the IAM gateway device, including [CPU usage], [Disk Usage], [Sessions], [WAN IP], [Flow Status], as well as [View Connection Ranking], [View Flow Ranking], [View Connection Monitoring] and [View Online Users].



[Note]: Displays various alarm, prompt information, etc.

[Flow Status]: Displays the received and sent data through the selected network interface card (NIC) interface, etc.

<View Connection Ranking>: Click this link to view the ranking information of the active

connections of the IAM gateway device and the detailed connection information of an IP address. For detailed introduction, please refer to Section 10.1.2 Connection Ranking.

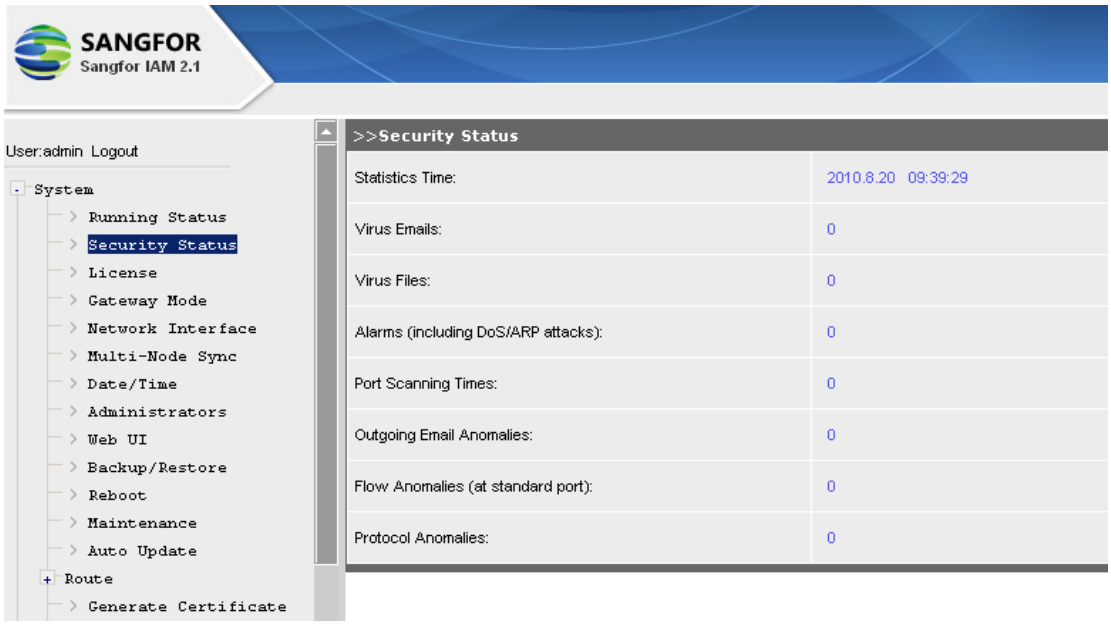
[View Flow Ranking]: Click this link to view the uplink and downlink flow information of the top 10 rankings, the IP group to which this IP address belongs, traffic amount of the uplink and downlink and of specific application. Click <Obtain> below the hostname, and you can get the device name corresponding to this IP address. For detailed configuration, please refer to Section 10.1.1 Flow Ranking.

[View Connection Monitoring]: Click this link to view the connection information. Enter an IP address and click the <Search> button, and you can get the current connection information of this IP address. For detailed configuration, please refer to Section 10.1.3 Connection Monitoring.

[View Online User]: Click this button to view the online user(s) verified by IAM gateway device, the login time and online duration of this user. The online user(s) can be forced to <Log Out> or <Block For> some time. For details, please refer to Section 7.7 Online User.

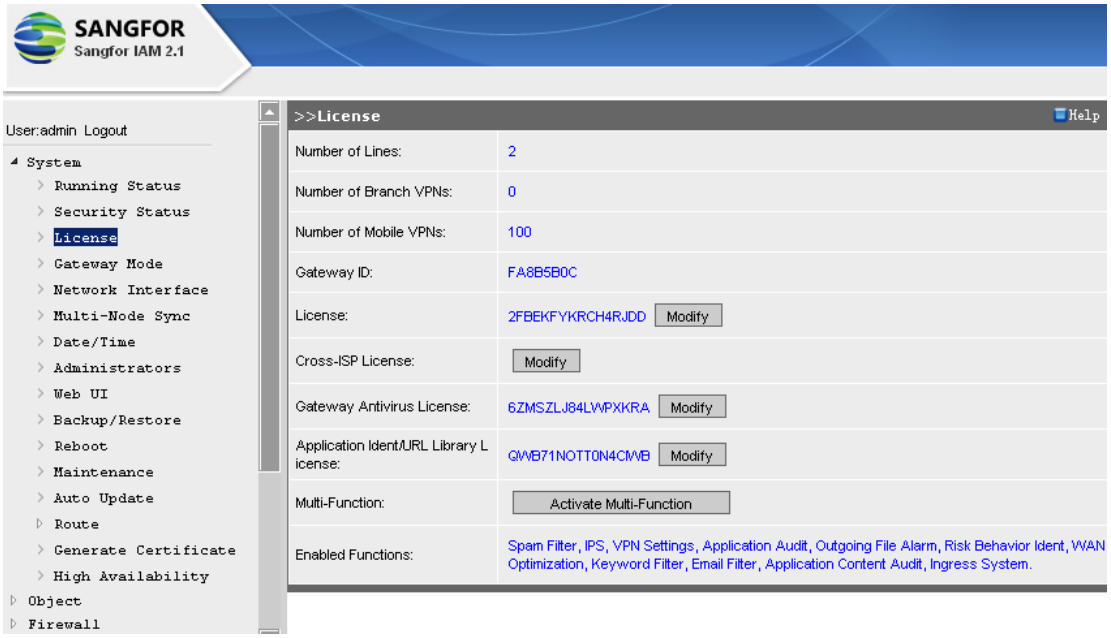
3.2. Security Status

[Security Status] displays the network security information and statistics of the IAM gateway device, including [Statistics Time], [Virus Emails], [Virus Files], [Alarms] (including DoS/ARP attacks), [Port Scanning Times], [Outgoing Email Anomalies], [Flow Anomalies] (at standard port) and [Protocol Anomalies]. The related page is as shown below:



3.3. License

[License] includes [Gateway Antivirus license], [Application Ident/URL Library License] and [Multi-Function] authentication, etc. It limits the number of connections from external networks, of Branch VPN and Mobile VPN. A different license supports a certain number of lines and VPN licenses. [Cross-ISP License], [Gateway Antivirus License], [Application Ident/URL Library License] and [Multi-function] are optional.



[Cross-ISP License]: You can activate it so as to be able to establish VPN crossing ISPs.

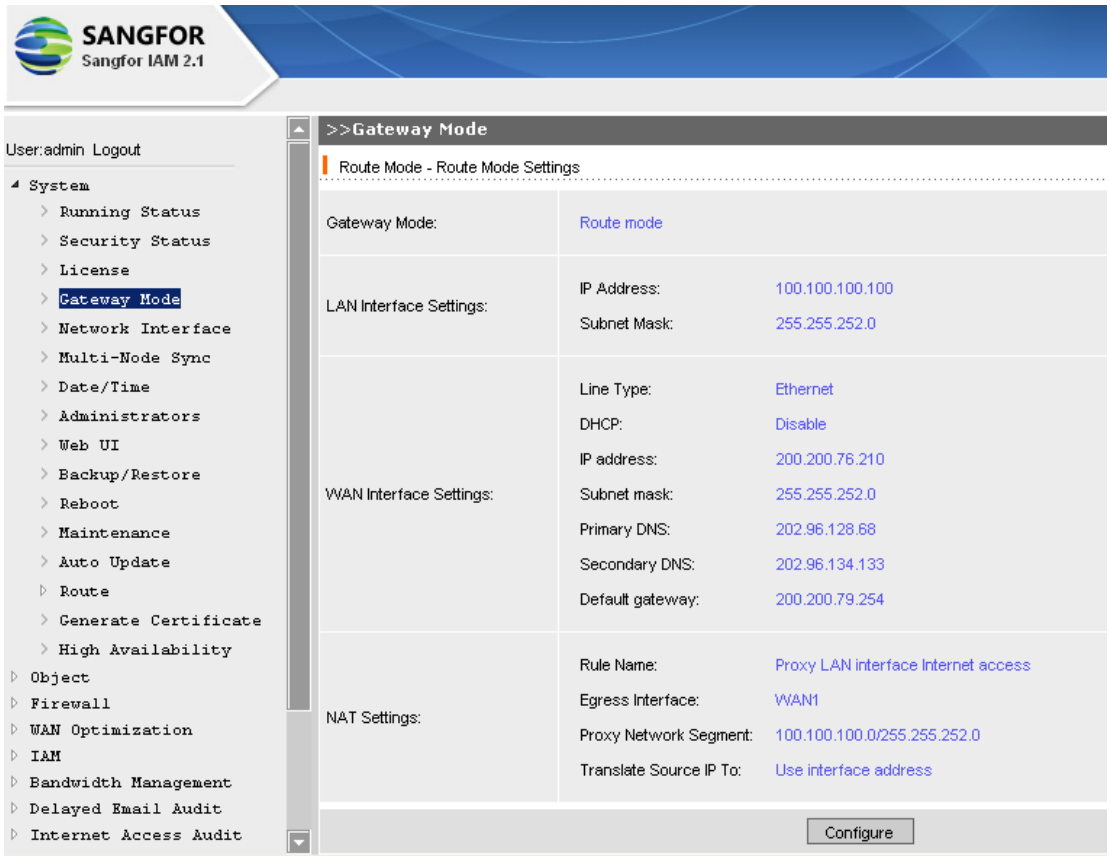
[Gateway Antivirus License]: You can activate it to update the virus library of the antivirus module.

[Application Ident/URL Library License]: You can activate it to update the expiry time of the application identification library and URL identification library

[Multi-Function]: Click the <Activate Multi-Function> button followed; enter the serial number, and then click the <OK> button to activate this function. Multi-function includes the following functions: Spam Filter, IPS (Intrusion Prevention System), VPN Settings, Application Audit, Data Center DKEY Search, Outgoing File Alarm, Risk Behavior Identification and SSL Identification. [Enabled Functions] indicates this device has activated the listed functions.

3.4. Gateway Mode

[Gateway Mode]: Configures the working mode of the IAM gateway device. Four working modes are selectable, namely, [Route Mode], [Bridge Mode], [Bypass Mode] and [Single-arm Mode]. The default configuration page of [Gateway Mode] is as shown below:



The current gateway mode and interface information are seen, below which is a <Configure> button.

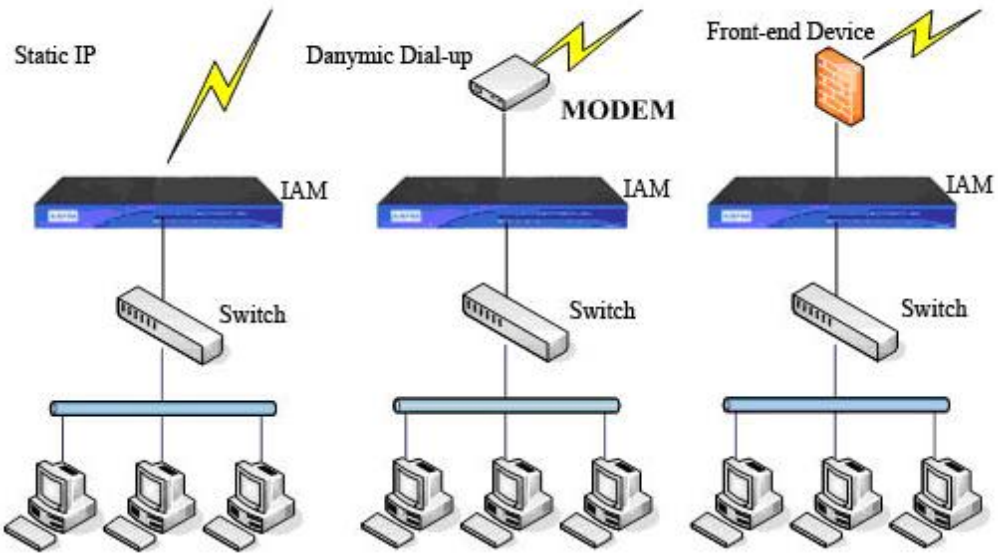
Click the <Configure> button to get into the next page and select the gateway mode to be switched to.

Click the <Next> button and finish the rest required configuration options.

3.4.1. Route Mode

[Route Mode] takes the IAM gateway device as a route device. The IAM gateway device is generally located at the exit of the LAN gateway, proxying the LAN users to get access to the Internet; or the IAM gateway device is located below the router which then proxies the LAN users to get access to the Internet.

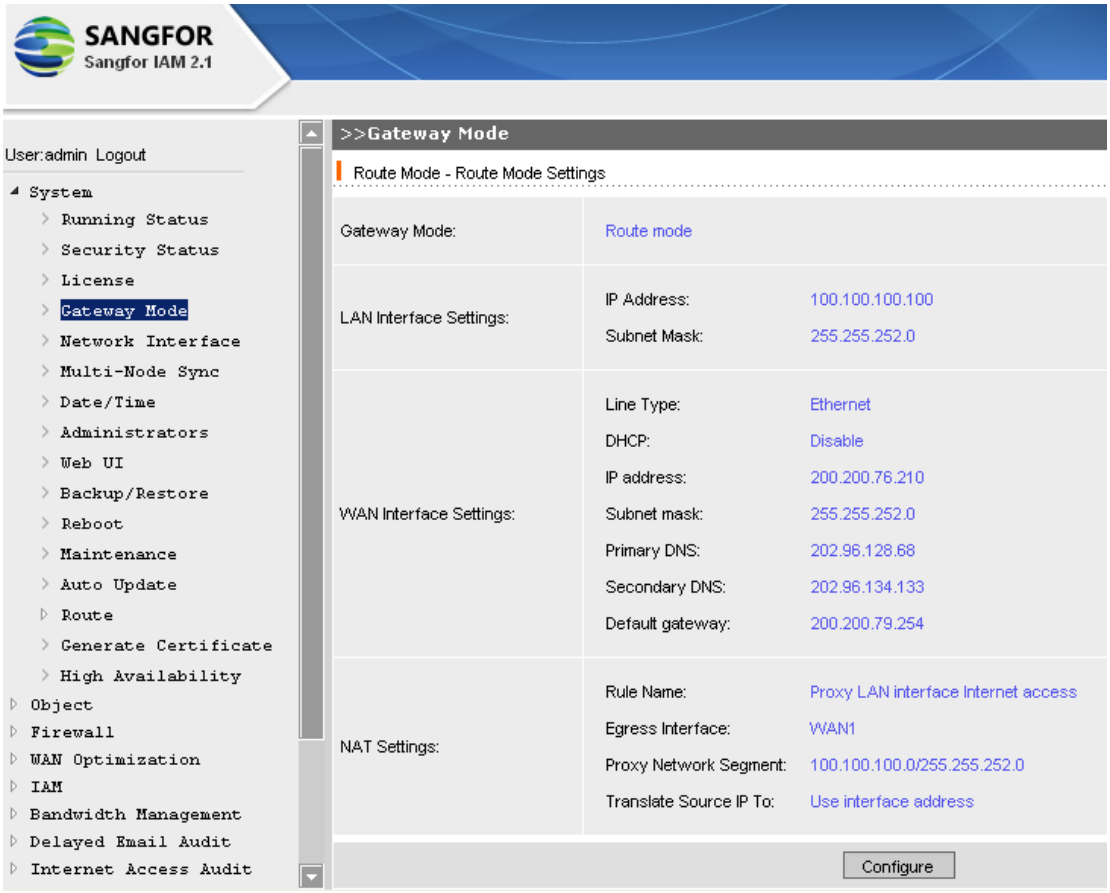
The deployment is as shown in the following figure:



Under Route mode, the default gateway of all the LAN servers are directing to the LAN interface IP of IAM gateway device, or to the layer 3 switch which then directs to IAM gateway device. The requests for Internet access are forwarded through the NAT function or the routing function of the IAM gateway device.

- LAN interface and WAN interface should be configured with an IP address respectively that is of different network segments.
- If WAN2 interface (on the front panel of the IAM gateway device) is not used, you can define WAN2 interface as a LAN2 or DMZ2.
- If the LAN interface of the IAM gateway device is configured with 802.1Q-VLAN address, the LAN can connect to the **TRUNK** interface of the layer 2 switch that supports VLAN, and the IAM gateway device can forward data between different VLAN(with single-armed route), besides, you can configure [LAN<->LAN] firewall rules. In other words, the access among different VLAN ID (VID) can also be controlled if the LAN interface is configured with 802.1Q-VLAN address.

The [Route Mode Settings] are as shown in the figure below:

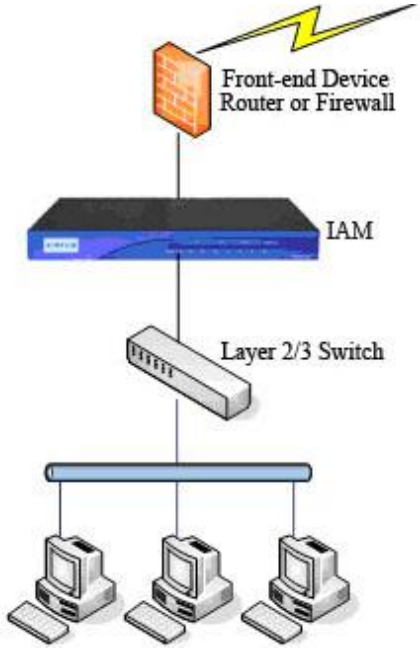


3.4.2. Bridge Mode

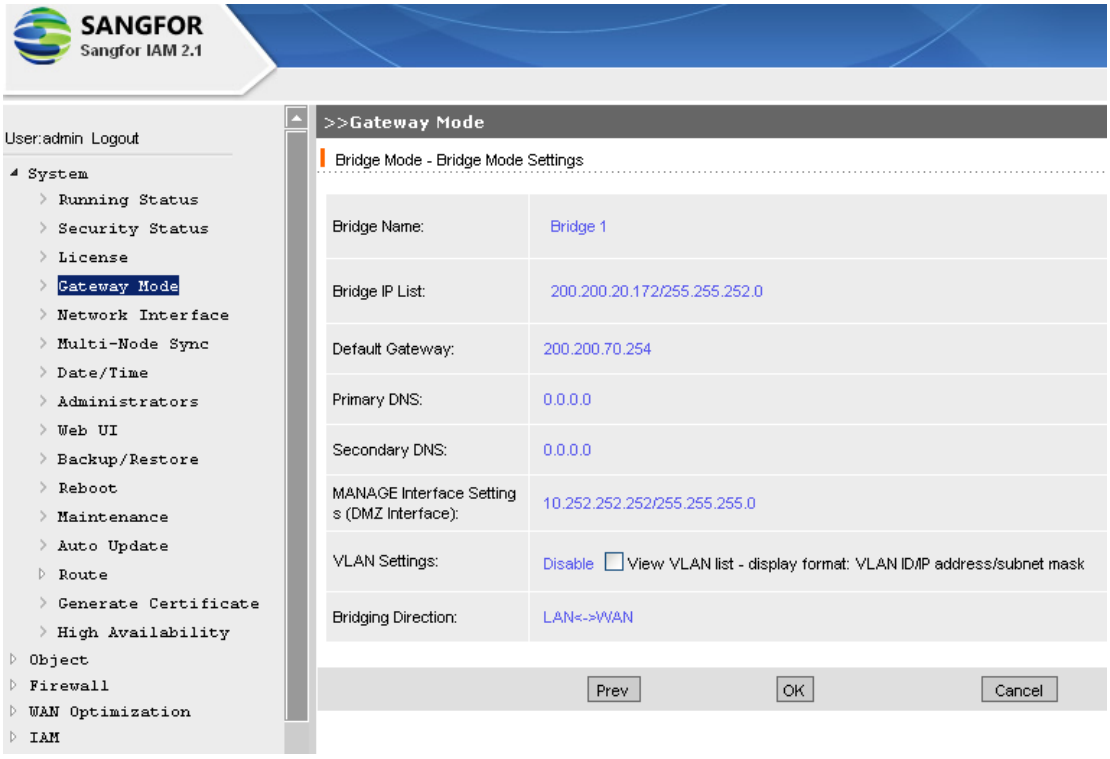
Bridge-mode deployment takes the IAM gateway device as a network cable with filtering function. This mode is usually applied where the original topology of the network is inconvenient to be altered.

The IAM gateway device locates between the original gateway and the LAN users, no change to be made on the original gateway and the LAN users. It seems the original gateway and the LAN server cannot feel the existence of the IAM device. It is what we call “Transparent” deployment for the original gateway and the LAN users.

Bridge-mode deployment features traversing the data of the data link layer, absolutely transparent to the users. Generally, if the IAM gateway is deployed as that shown in the following figure, Bridge mode is recommended.



The configuration page is as shown below:

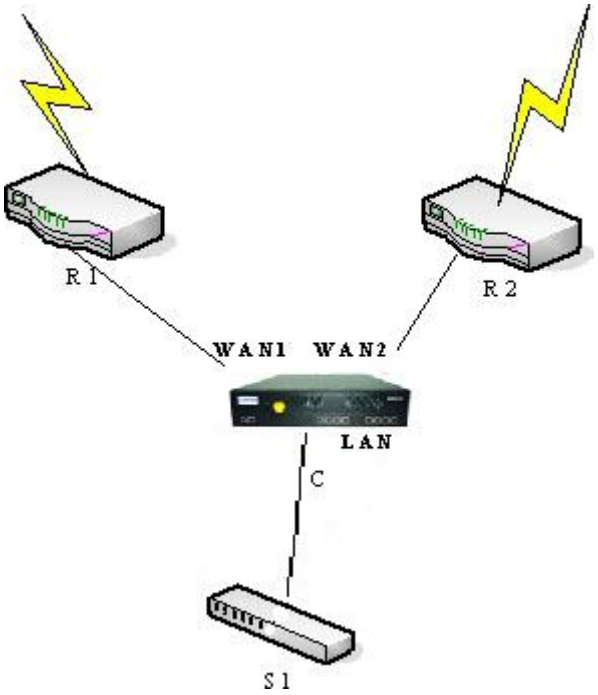


3.4.2.1. Bridge Mode: Multiple-Interface

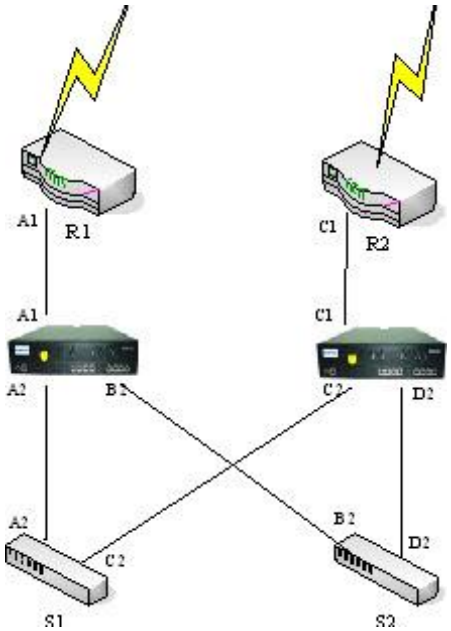
Through bridging the interfaces of the IAM gateway device, we can establish multiple interfaces for a bridge so as to create an environment supporting dual routes or dual lines of the network.

Environment examples for Bridge-mode deployment:

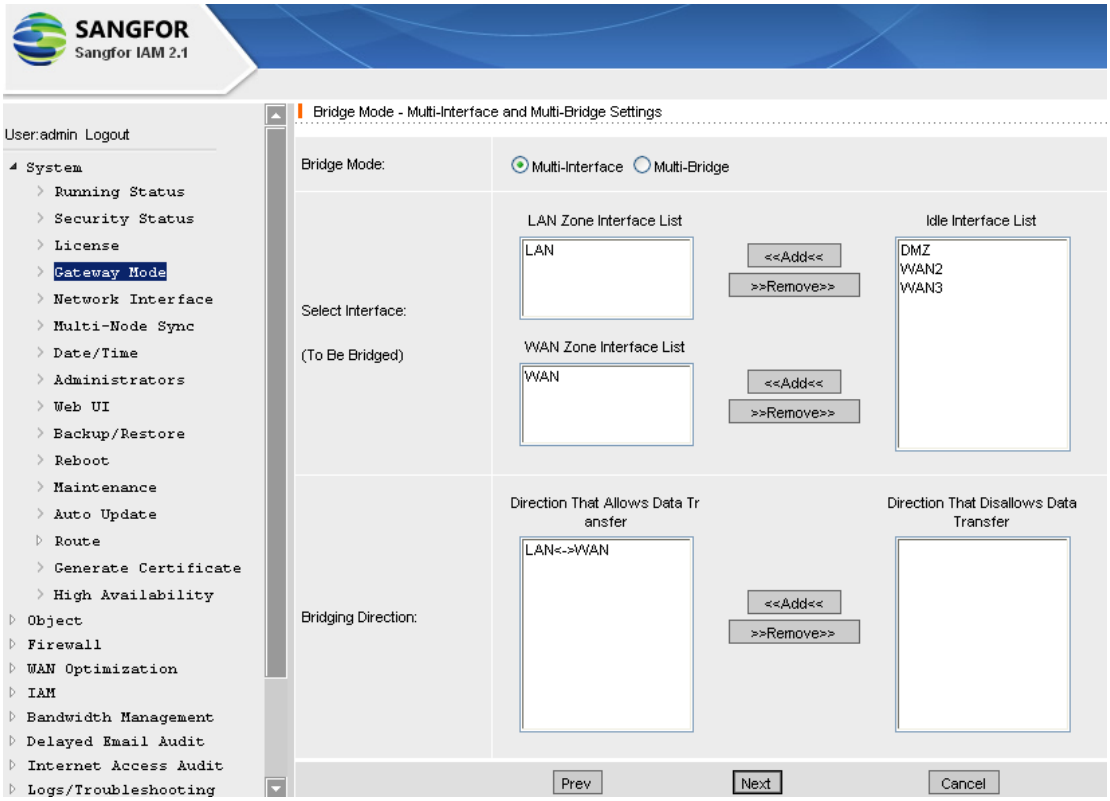
Environment 1: S1 connects to two external lines R1 and R2; an IAM gateway device (under bridge mode) is then deployed to bridge R1 and R2 with S1.



Environment 2: In order to enhance the stability of the network and reduce single-node failure, both the kernel switch and the router of local area network are in redundancy. Then we deploy two IAM gateway devices into the networking, as shown in the following figure:



The configuration page of [Bridge Mode- Bridge Mode Settings] is as shown below:



[Gateway Mode]: Options are [Multi-Interface] and [Multi-Bridge].

[Select Interface]: Only available for [Multi-Interface].

[LAN Zone Interface List]: The selected interface will connect to local area network.

[WAN Zone Interface List]: The selected interface will connect to the outgoing device(s).

[Bridge Direction]: Defines the direction the data forwarded from and being forwarded to. In association with the settings of the firewall rules, this item can allow or deny data transmission of certain direction.

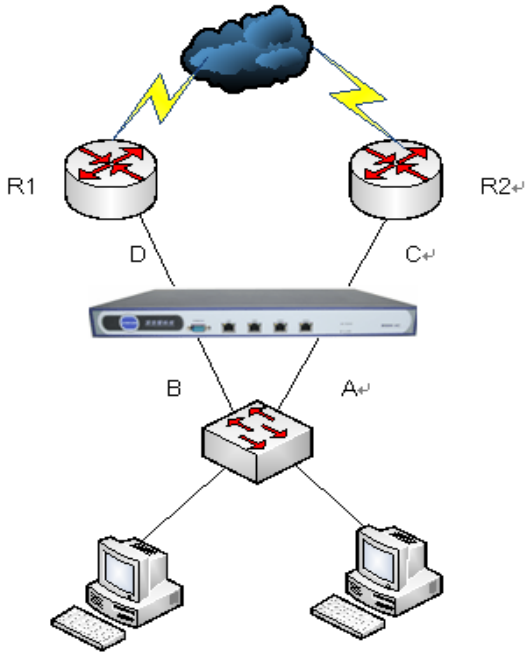
Differences between Multi-Interface and Multi-Bridge: Multi-Interface indicates one bridge has several interfaces, and the IAM gateway device maintains only one MAC address table; while Multi-Bridge regards that inside the IAM gateway device there are two independent bridges, each individual bridge maintaining its own MAC address table, and the data of the two bridges cannot be forwarded to each other.

3.4.2.2. Bridge Mode: Multi-Bridge

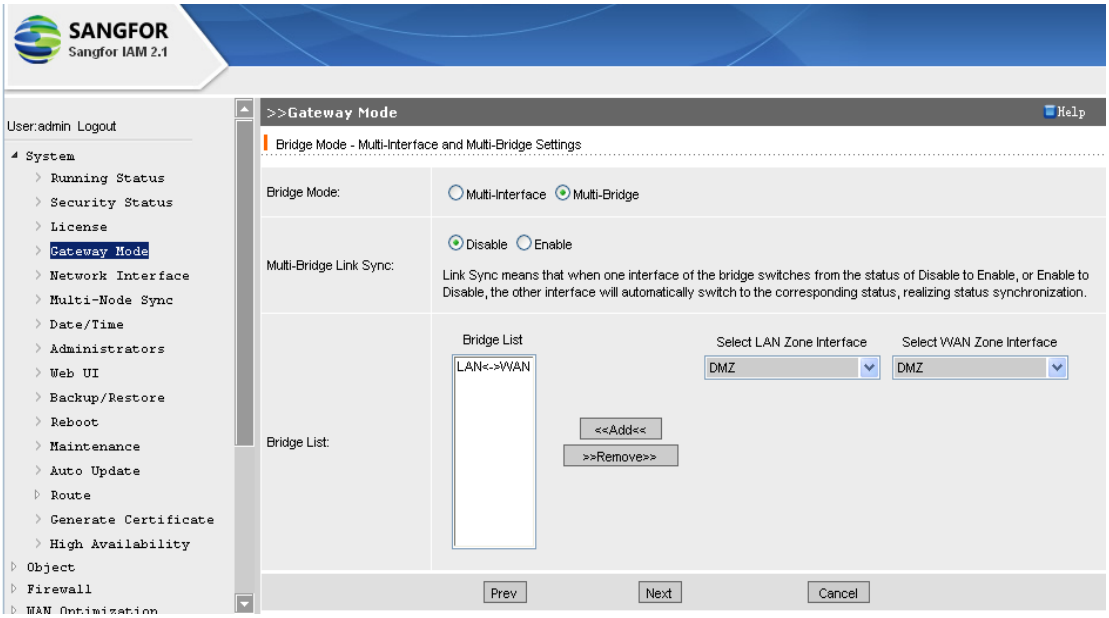
Environment for Bridge mode Multi-bridge:

In order to enhance the stability of the network and reduce single-node failure, both the kernel switch and the router of local area network are in redundancy. Both R1 and R2 use VRRP protocol. When the host is down, the alternate device enables the virtual IP and takes over the network. Then we deploy the IAM device in Multi-Bridge Mode, data transmission directions are A→C, B→D (corresponding to those in the Bridge list).

Detailed deployment is as shown in the following figure:



The configuration page is as shown below:

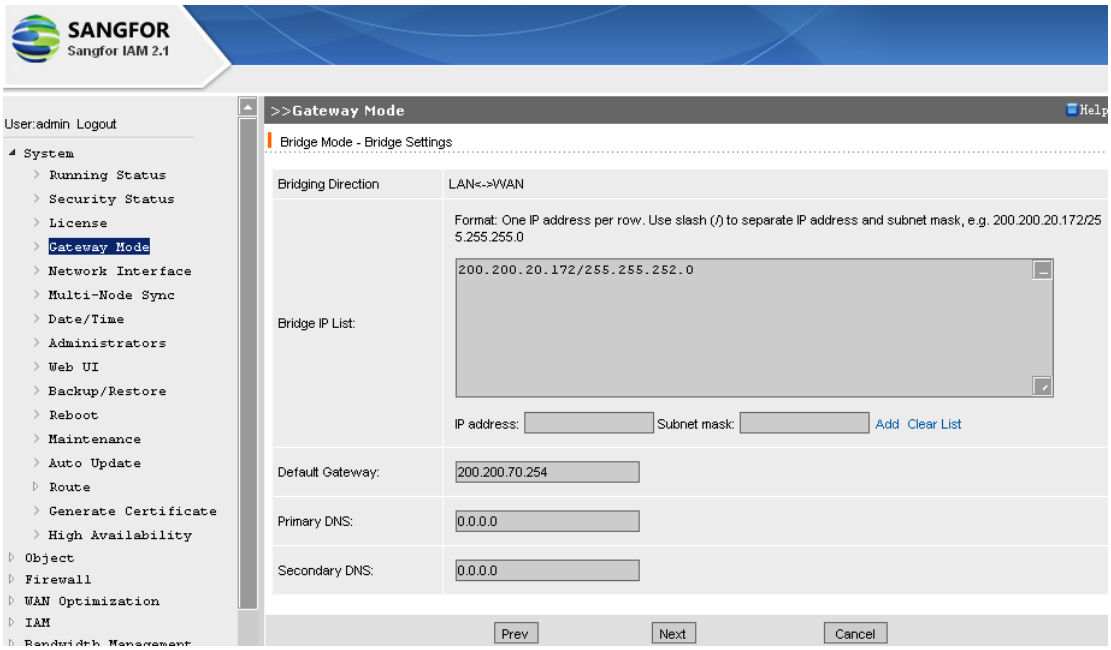


[Select LAN Zone Interface]: Select a LAN interface.

[Select WAN Zone Interface]: Select a WAN interface.

[Bridge List]: Defines the direction the data are forwarded to.

Click the <Next> button to get into the next page to configure the bridge, as shown below:



[Bridge Direction]: Indicates the direction of data transmission.

[Bridge IP List]: Based on [Bridging Direction], configures the IP interface of the LAN interface. As to different bridging directions, the Bridge IP can be of a same network segment.

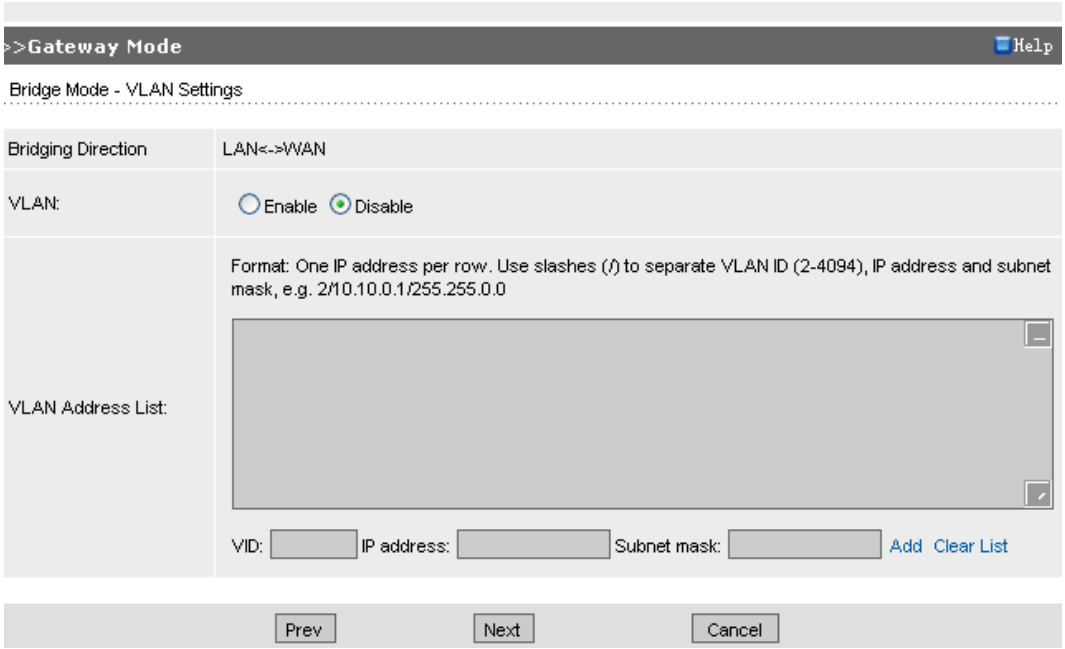
[Default Gateway]: Directs to the next hop interface IP of the bridge.

Under Multi-Bridge mode, you have to configure [Default Gateway] for each bridging direction. [Default gateway] configures the default route of each bridge that is directing to the gateway.

- Under Bridge mode, gateway of the LAN PC needs no other change, but remains directing to the original gateway, in other words, LAN PC directs to the LAN interface IP address of the front-end device.
- Under Bridge mode, the data for Internet access should be ensured to pass through IAM gateway device, that is, the LAN user must not bypass the IAM gateway device and follow the physical line of the original gateway to get access to the Internet.
- As to data traversing, please ensure the WAN zone connects to the front-end routing device and the LAN zone connects to the LAN switch. These two connections cannot be mixed up. The data for Internet access transmitted from LAN zone to WAN zone can be monitored and controlled.
- "Transparency" of bridge-mode IAM gateway device is achieved at the data link layer (the second layer of OSI), interfaces of the device are being bridged; the data of layer 2 and the layers above can be traversed. This feature of the IAM gateway device enables the DHCP service and the IP/MAC binding (of the original gateway) work.
- NAT function is unavailable in Bridge mode.
- Under Bridge mode, VPN module on the local IAM gateway device is unavailable.
- If you want to enable the anti-virus function, email filter, etc., or if you want to have the URL library, application identification library and virus library automatically updated, you need to configure the [Bridge IP List], [Default Gateway] and [DNS], and make sure the IAM gateway device itself to get access to the external network (you can implement "ping" to check the availability of the external network).
- If you want to enable the WEB authentication, ingress rule or other functions that need to be redirected to the IAM gateway device and there are several LAN segments, you must add a corresponding route, directing to the routing device.
- If the computers of layer 2 switch have multiple network segments (instead of VLAN), the gateway should also have IP addresses of multiple segments. If so, and you want to enable the functions that need to be redirected to the IAM gateway device, such as anti-virus function, email filter, ingress rule, WEB authentication, etc., the IP addresses of these

network segments should also be configured in [Bridge Mode] > [Bridge Settings] page > [Bridge IP List].

- Under Bridge mode, the IAM gateway device supports VLAN TRUNK traversing; [Bridge IP] can be IP address of 802.1Q-VLAN (which indicates the IAM gateway device can be transparently connected to the main channel of VLAN TRUNK). To configure the Bridge-mode deployment to support VLAN TRUNK, go to [Gateway Mode] > [Bridge Mode] > [Bridge mode -VLAN Settings] page, as shown below:

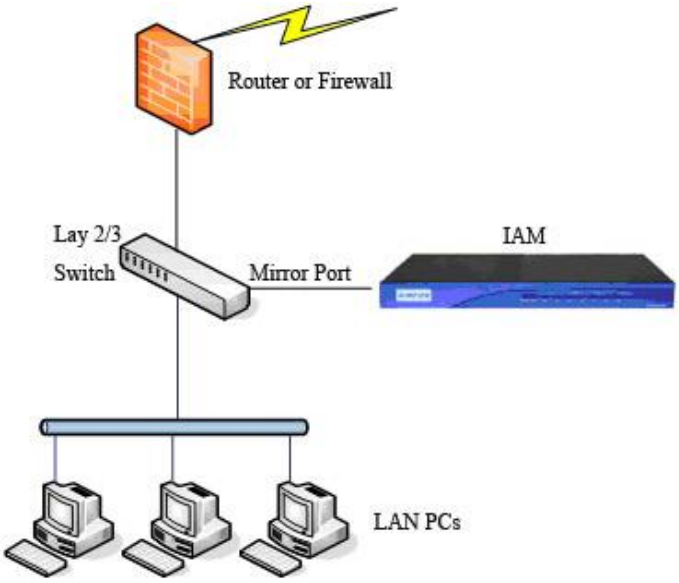


Enter [VID], the VLAN [IP address] and [Subnet mask], and then click <Add>. If you have enabled the functions that need to be redirected to the IAM gateway device, such as anti-virus function, email filter, ingress rule, WEB authentication, etc., you have to configure this IP address; otherwise, you can also leave the VLAN address list blank.

3.4.3. Bypass Mode

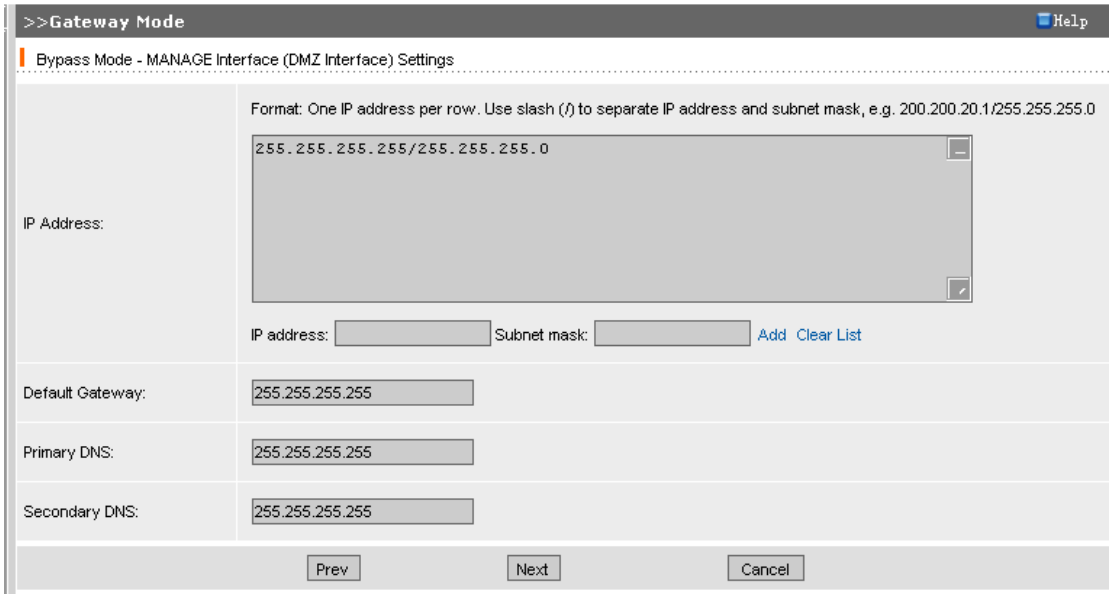
Without altering the networking, bypass-mode IAM gateway device can fulfill monitoring and controlling, and can avoid disconnecting with the users. The IAM gateway device is connected to the mirror port or the HUB, monitoring the overall local area network. Bypass mode plays no influence on the network environment, and device failure will not disconnect the network.

Typical topology of bypass-mode deployment is as shown below:



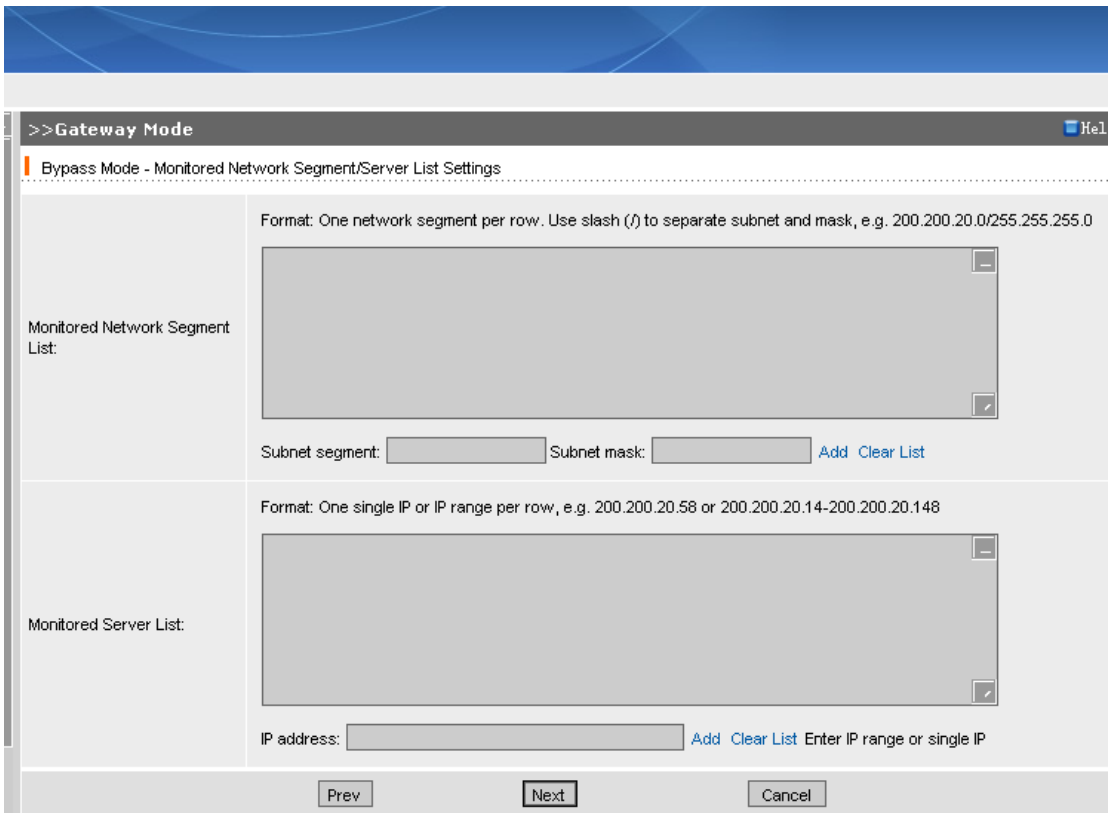
Under the [Gateway Mode] default configuration page, click <Configure> to enter the [Select Gateway Mode] page.

Select [Bypass Mode] and click the <Next> button, then the following page appears:



[IP Address]: Configures the IP address of the MANAGE interface (DMZ interface).

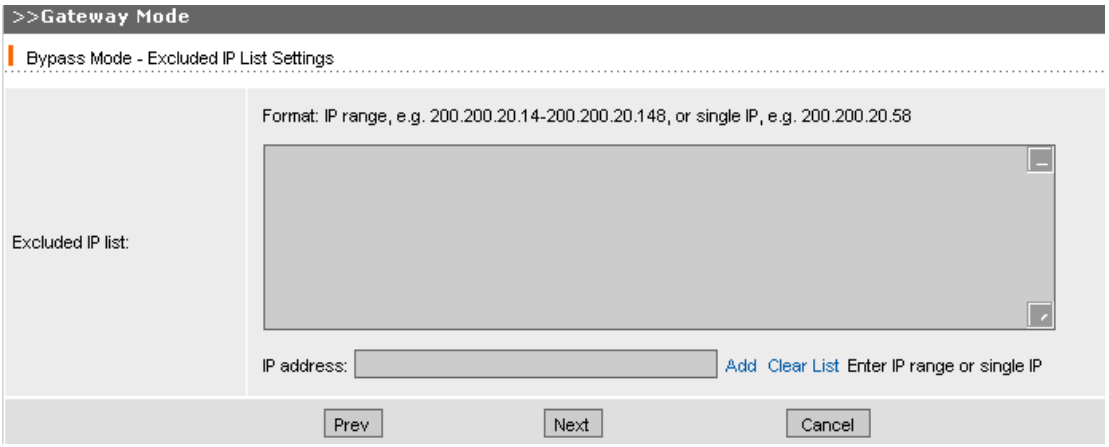
Click the <Next> button to get into the next configuration page, as shown below:



[Monitored Network Segment List]: Configure the network segments to be monitored.

- In order to have the IAM gateway device connecting to the console or the client-updater, the [IP Address] and [Default Gateway] must be configured and the network cable should connect to the DMZ interface.
- Since bypass-mode IAM gateway mode needs only one network cable to connect the LAN interface or WAN1 (of the IAM device) to the HUB or mirror port of the switch, IAM gateway device has no knowledge of which addresses are LAN addresses or which addresses are WAN addresses, but regards the addresses in the [Monitored Network Segment List] as LAN addresses. Access data sent to the Internet through these monitored addresses will be recorded or controlled. However, IAM gateway device will default not to record the access between two LAN PCs, which means, communication between any of the two addresses in the [Monitored Network Segment List] will not be monitored.
- Also, access data sent to the Internet through the server(s) of the [Monitored Server List] will be recorded or controlled. Different from [Monitored Network Segment List], the access data sent by the network segment(s) and passing through the LAN servers will be recorded.
- The data irrelevant to the addresses or severs in the above two lists will not be monitored.

Click the <Next> button to continue the next step, configuring [Excluded IP List], as shown below:



[Excluded IP List]: Access data requested by these excluded IP addressed will not be recorded.

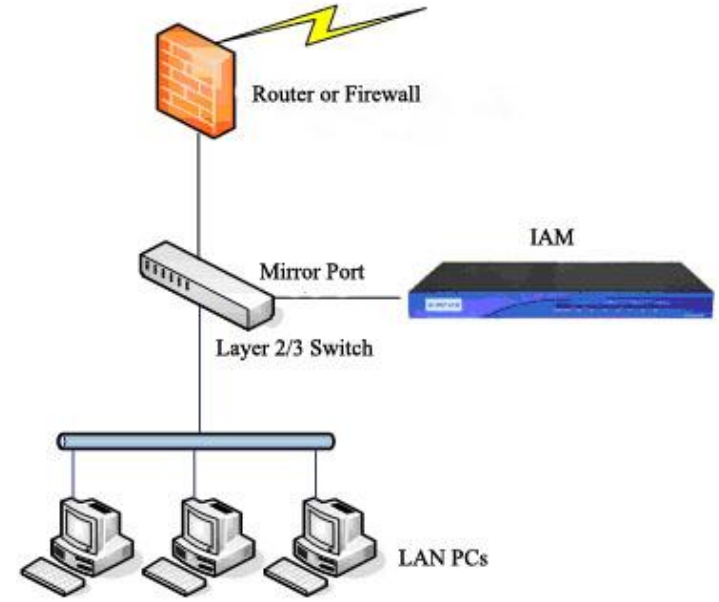
- Bypass mode deployment supposes that there is a HUB or a switch with mirror port. If the switch has no mirror port, please connect a HUB to the front end of the switch.
- Under Bypass mode, <View Flow Ranking> and <View Connection Ranking> are unavailable.
- Under Bypass mode, TCP control is fulfilled by sending 'reset' packets through the DMZ interface. Therefore, to achieve TCP control, all the 'reset' packets sent through the DMZ interface must be ensured to be received by the PC and the server of the public network.
- Many functions are not available in bypass mode, such as VPN, DHCP and Ingress rule, etc.
- Bypass-mode IAM gateway mode mainly plays a monitor role; control functions are not as complete as those of Route mode or Bridge mode, for it can only restrict some TCP connections, such as URL filtering, keyword filtering, email filtering, etc. No UDP connection control can be done, such as P2P software, QQ login, etc.

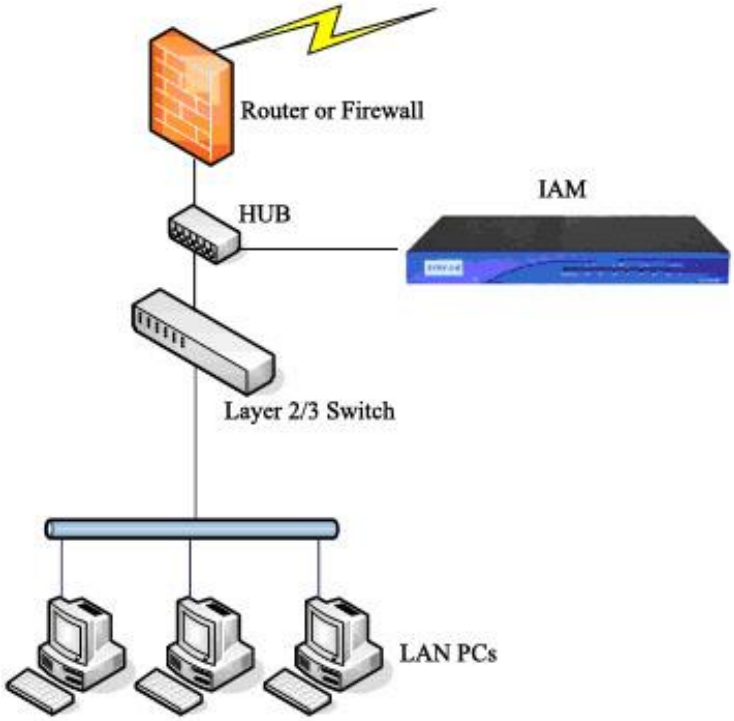
3.4.4. Single-Arm Mode

Single-arm-mode deployment takes the IAM gateway device as a proxy. IAM gateway device can fulfill monitoring and controlling, and can avoid disconnection of the users with the Internet. The IAM gateway device is connected to the HUB or the mirror port of the switch, monitoring the overall local area network. Single-arm mode requires no change on user's networking and plays

no influence on the network environment. If the device is down, you need only disable the proxy service on the user's PC and to have it back into normal.

Typical topology of the single-arm mode is as shown below: failure will not disconnect the network.

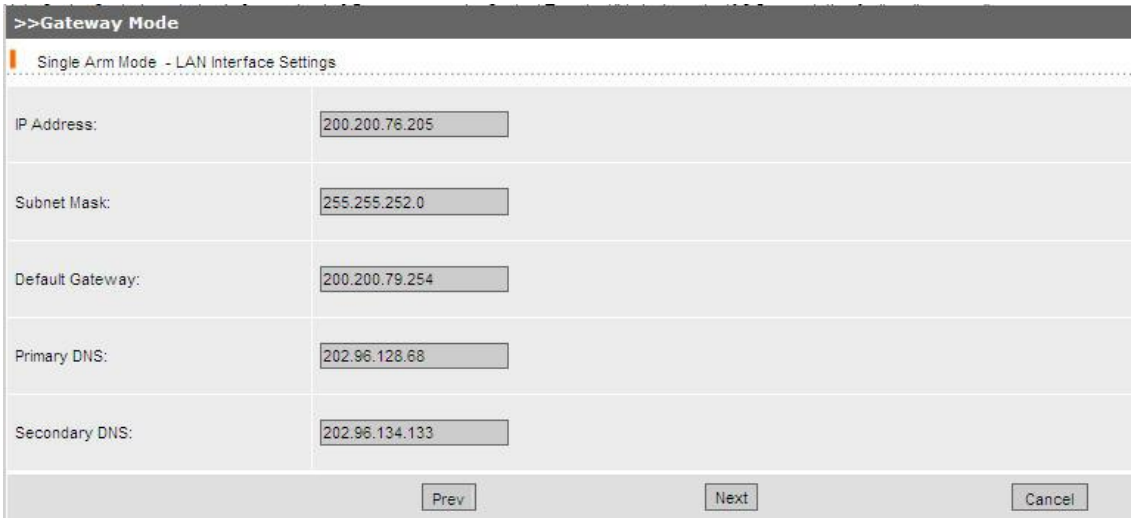




Under the [Gateway Mode] default configuration page, click <Configure> to enter the [Select

Gateway Mode] page.

Select [Single Arm Mode] and click the <Next> button, then the following page appears:



[IP Address]: Configures the IP address of the LAN interface.

[Default Gateway]: Configures the gateway of the local area network, same with the gateway of the LAN computer.

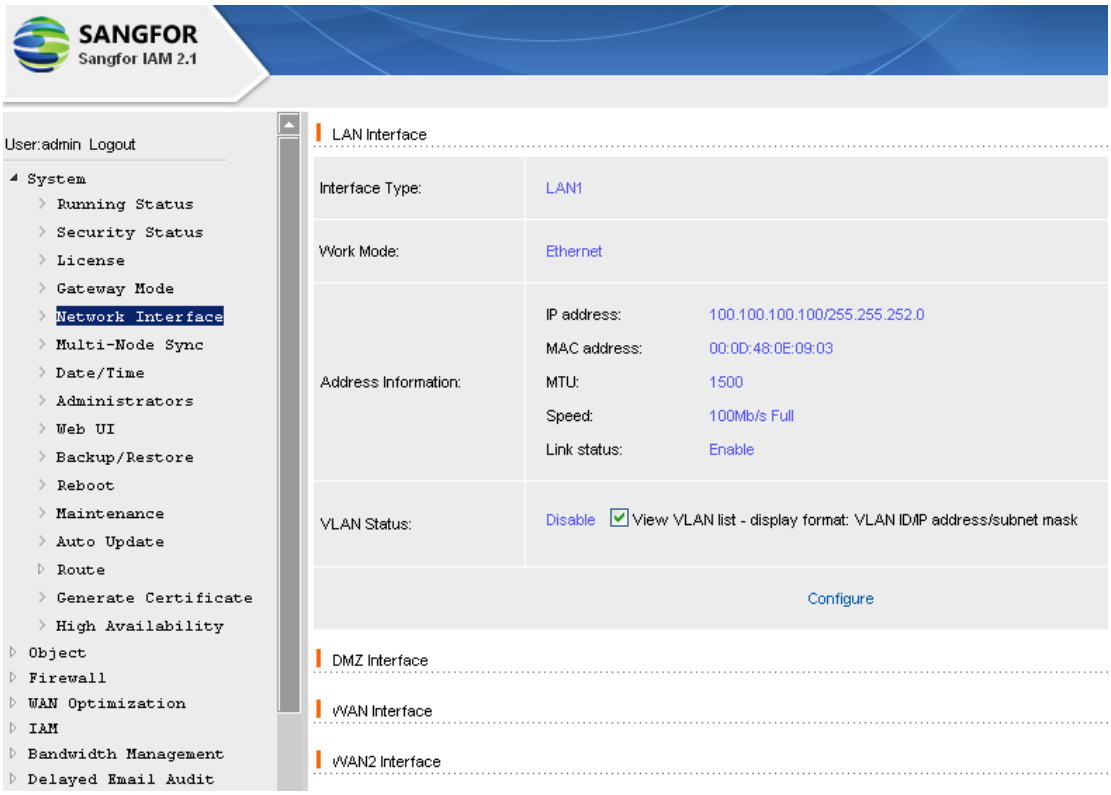
Click the <Next> button to get into the next configuration page, as shown below:

- Under single arm mode, the gateway configured in the local area network need no change, keeping directing to its original gateway.
- To have the IAM gateway device work in single arm mode, you have to configure the [WAN Optimization] > [Proxy Options].
- VPN is not available for single arm mode.
- Single mode mainly functions as a proxy. If a LAN user needs to get access to the Internet, it need only have its computer's proxy server direct to the IAM gateway device, proxy server address being set as the LAN interface IP address and the port as the proxy port (configured in [WAN Optimization] > [Proxy Options] > [WAN Optimization] page).

3.5. Network Interface

Under Route mode, you can configure the network interfaces on this [Network Interface] page. If it is in Bridge mode, [Multi-bridge], you can also configure the bridge here. As to other gateway modes, the network interfaces are configured in [System] > [Gateway Mode].

[Network Interface] default configuration page is as shown below:



[LAN Interface]: Displays the information of LAN interface. Click the <Configure> button to enter the corresponding configuration page.

If you are to configure multiple IP addresses, you can add the IP addresses that are to be bound; click the <Next> button to get into the next page.

[VLAN]: [Enable] or [Disable] VLAN.

[VLAN Address List]: If the interface of the switch that is connecting to IAM gateway device has applied Trunk, then configure the IP address and VID (VLAN ID) for the VLAN at the LAN interface.

The VLAN function supports VLAN (802.1Q) networking environment. If the LAN interface of the IAM gateway device is configured with 802.1Q-VLAN address, the LAN can connect to the **TRUNK** interface of the layer 2 switch that supports VLAN, and data of different VIDs can be

forwarded to each other (one-armed route); besides, you can configure [LAN<->LAN] firewall rules to control the access among different VLAN IDs (VID).

[DMZ Interface]: Displays the information of DMZ interface. Click the <Configure> button to enter the corresponding configuration page to configure the [IP address] and [Subnet mask].

[WAN Interface]: Displays the information of WAN interface. Click the <Configure> button to enter the corresponding configuration page and configure the Internet access mode. If there is a second external line, define WAN2.

[WAN2 Interface]: Displays the information of WAN interface. It can be defined as the second external line, as well as a LAN interface or DMZ interface.

[WAN3 Interface]: Displays the information of WAN interface. It can be defined as the third external line, as well as a LAN interface or DMZ interface.

[Multiline Settings]: Displays the line selection policy selected. Click the <Configure> button to get into the configuration page and alter the line selection policy. Four policy options are available, with explanations above them. [Multiline Settings] is suitable for the networking that consists of multiple external lines.

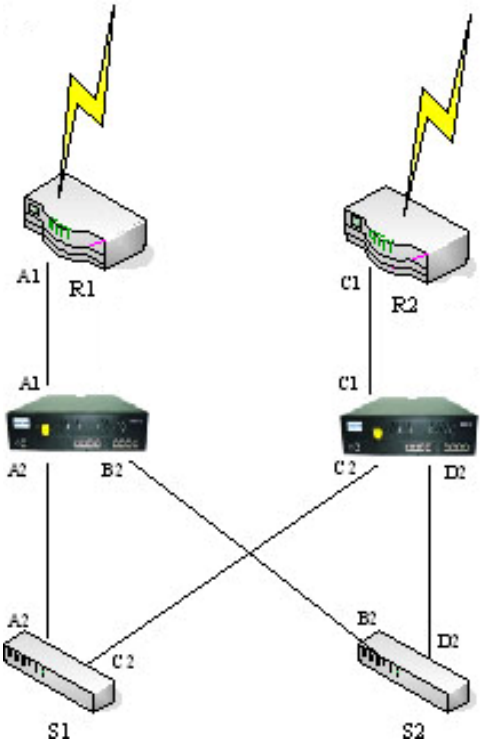
3.6. Multi-Node Sync

Environment for multi-node synchronization:

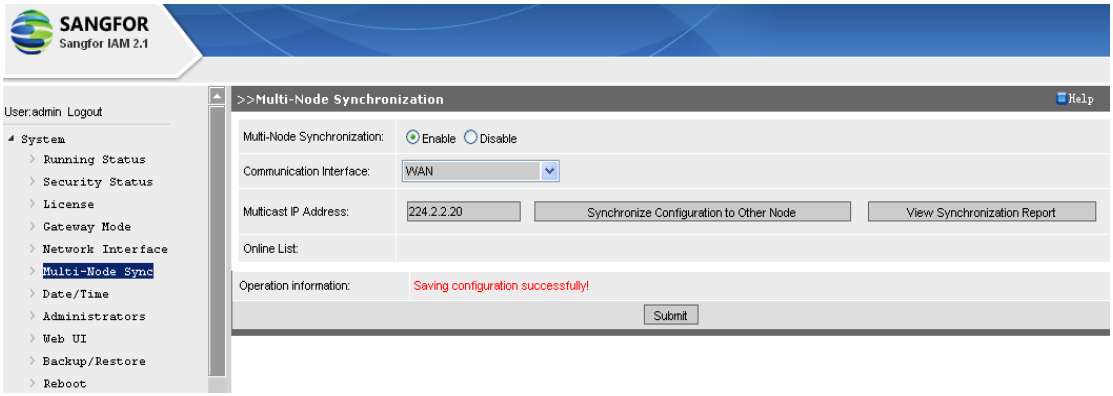
Two IAM gateway devices, A and B, are located in the local area network. Both of them work in Bridge mode. Internet access requests of the LAN users pass through device A or B; user information and access control policy are configured on IAM gateway device A.

Requirement: IAM gateway device A synchronizes IAM gateway B with the user information in real time.

The deployment of multi-node system is as shown below:



The [Multi-Node Synchronization] configuration page is as shown below:



[Multi-Node Synchronization]: [Enable] it and the user authentication information, user list, and data of the internal identification libraries will be synchronized in real time.

[Communication Interface]: Configures the network interface used for the synchronization between the IAM gateway devices. The communication interface can be any network interface that can cross multicast packets to communication with each other. It is recommended to use an idle network interface to connect them directly.

[Multicast IP Address]: Configures the multicast address used for synchronization between the IAM gateway devices. The multicast can be any addresses of the multicast IP range. However, the multicast IP addresses configured on the to-be-synchronized IAM gateway devices must be the same.

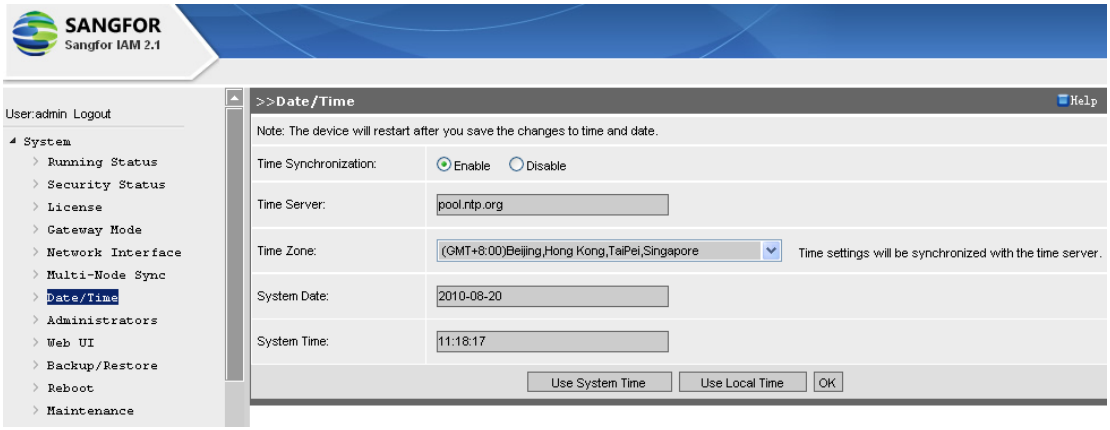
[Online List]: Displays the IP addresses of the synchronization-related devices.

Having completed configuring the page, you have to click the <Synchronize Configuration to Other Node> button to send synchronization signals to the other node (IAM gateway device); or click the <View Synchronization Report> button to view the synchronization information.

3.7. Date/Time

[Date/Time]: Configures the system date and time of the SANGFOR IAM hardware gateway device. In addition to modifying the system time directly, you can configure a [Time Server] to synchronize the time, and select a local [Time Zone].

The configuration page is as shown below:



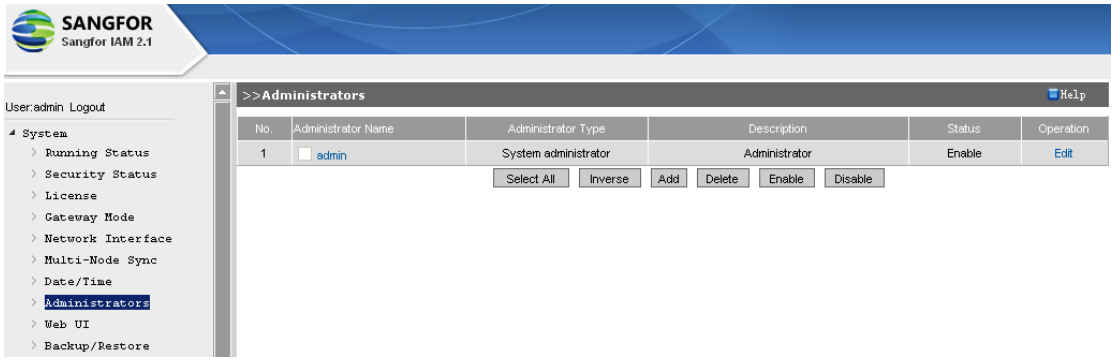
<Use System Time>: Click this button to update the time of the IAM gateway device.

<User Local Time>: Click this button to update the system date/time of the IAM gateway device with the date/time of the local PC with which you have logged in to the console of IAM gateway device.

Having completed configuring this page, you have to click the <OK> button to save all the settings.

3.8. Administrators

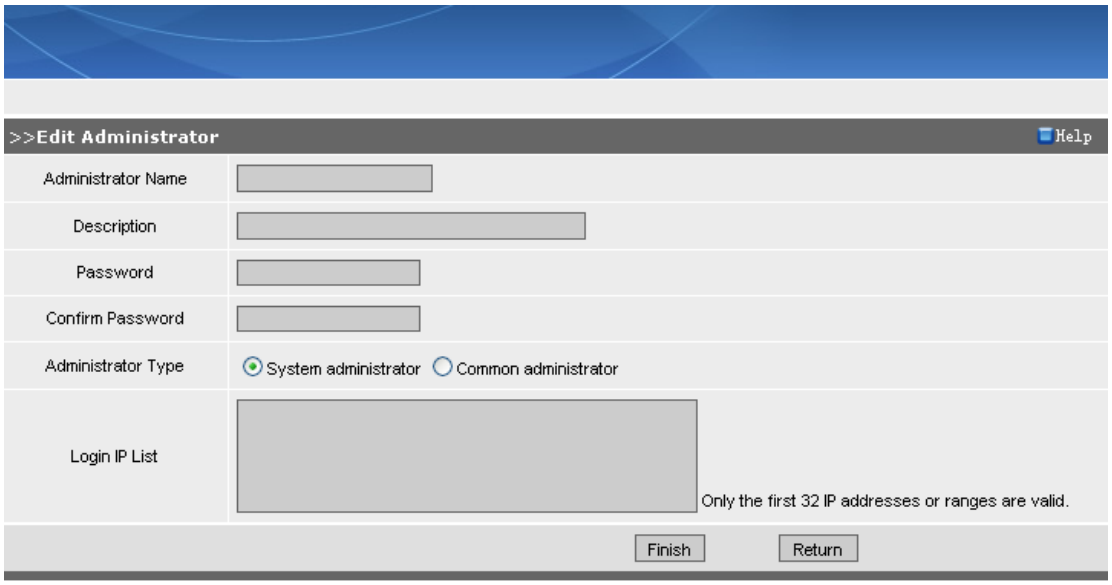
[Administrators] configures the console login user(s) who can manage the IAM gateway device through the console.



<Select All>, <Inverse>: Click the corresponding button to select the needed administrator(s).

<Delete>, <Enable>, <Disable>: Click the corresponding button to delete, enable or disable the selected administrator.

<Add>: Click this button to enter the [Edit Administrator] page, as shown below:



[Administrator Name]: Type in a unique name for this administrator to distinguish it from others.

[Description]: Type in a brief description for this administrator.

[Password]: Configures the login password for this administrator.

[Administrator Type]: Defines the role of the administrator, [System administrator] or [Common administrator].

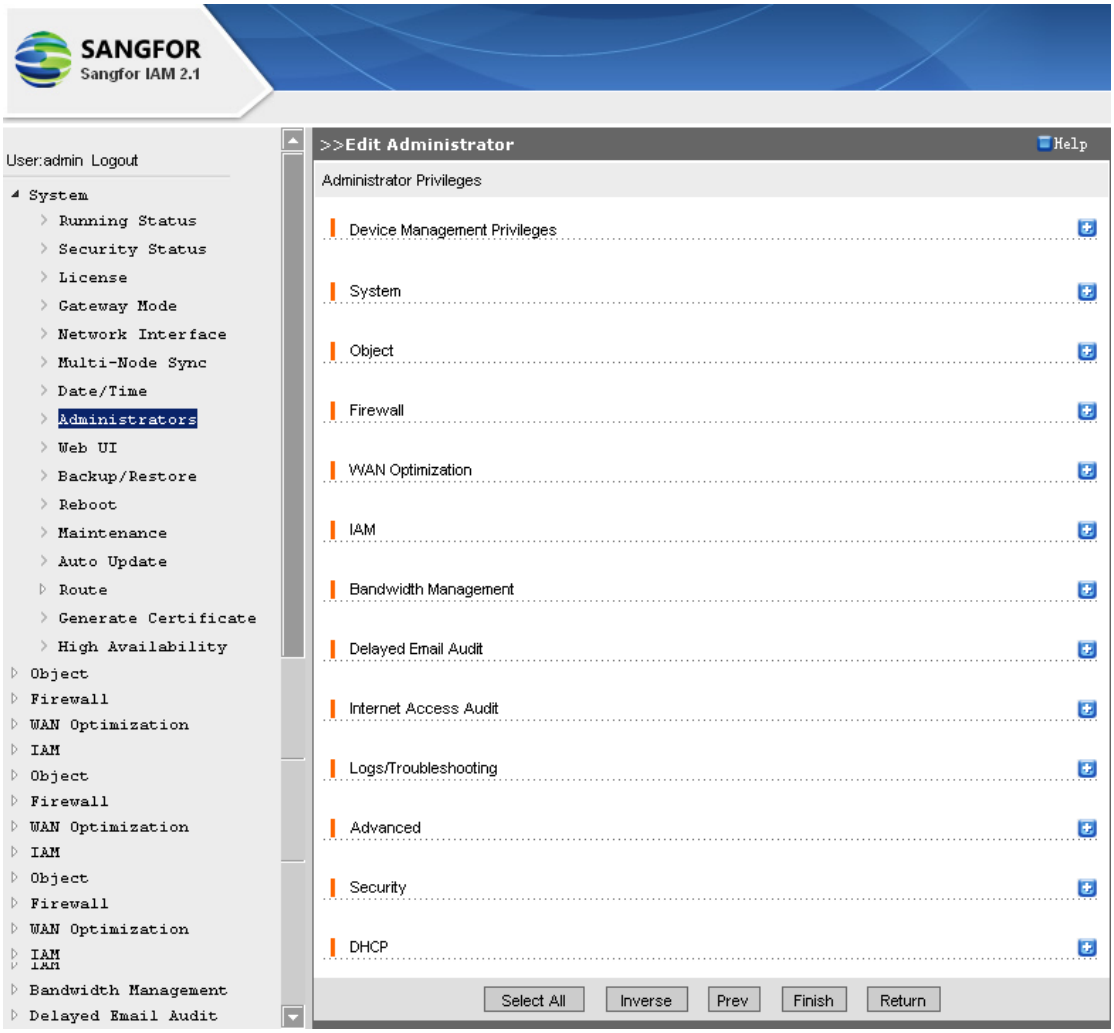
[System administrator] has all the privileges and can manage all the functions and user groups.

[Common administrator]'s privileges of managing is defined in much more details. More

introductions are followed in this section.

[Login IP List]: Configures the IP address(es) with which administrator(s) can log in to the console. You can type in a single IP address or IP range. One entry per line, maximum 32 entries are allowed.

Privilege configuration of [Common Administrator] is as shown below:



Privileges of common admin are divided according to functions module, there are privileges on [Device Management], [System], [Object], [Firewall], [IAM], [Bandwidth Management], [Delayed Email Audit], [Internet Access Audit], [Logs/Troubleshooting], [Advanced], [Security] and [DHCP].

[Device Management]: Configures the privileges the administrator have on managing the selected user groups. Click the <Select> button to browse the organization structure of the IAM gateway; click a user group or sub-group to add it to the list.

[Device Management Privileges] are, [View], [Member Management], [Policy Management],

[Delayed Email Audit] and [Data Center Audit].

[View]: Indicates this admin can only view the selected user or sub-group user information, viewing the policy applied to its group and the online user list.

[Member Management]: Indicates this admin can manage and edit the selected group and sub-group user. Once it is checked, it defaults with the [View] privilege and the privilege to block online user(s).

[Policy Management]: Indicates this admin can manage the selected group and sub-group user. Once it is checked, it defaults with the [View] privilege.

[Delayed Email Audit]: Indicates the admin can audit the delayed emails of the selected group(s). It is applicable to different user groups.

[Data Center Audit]: Indicates the admin can log in to the internal Data Center to view the logs of the selected group(s). The options of [Data Center Privileges] can be configured individually, which are [System Management], [Customized Report] and [Intelligent Report].

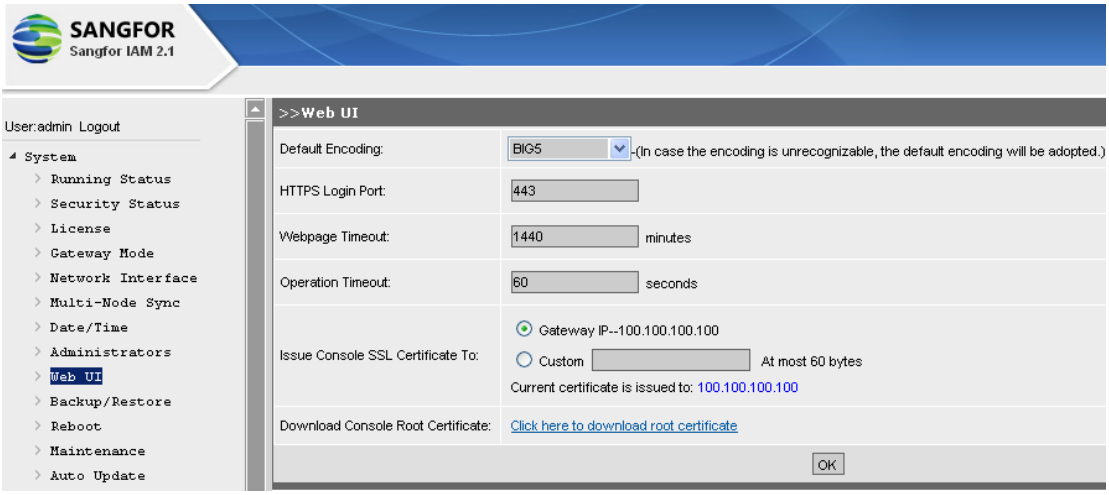
As to [System] and [Object] function modules, you can check [Edit Privilege] and [View Privilege].

- [Policy Management] only allows the administrator to edit the association relationship between the group/user and the po1icy. The policy itself cannot be modified, unless the admin is the administrator who has created this policy or a system administrator.
- If an administrator has neither the privilege to view nor the privilege to edit a certain function module, this module will not display on the left tree of the console, in other word, it is unavailable.

3.9. WEBUI

[WEB UI] configures the [Default Encoding], [HTTPS Login Port], [Webpage Timeout], [Operation Timeout], [Issue Console SSL Certificated to], [Download Console Root Certificate].

The configuration page is as shown below:



[Default Encoding]: Select an option and the unrecognizable codes of the monitored data will be handled as this code.

[HTTPS Login Port]: Configures the port of HTTPS protocol for logging in to the WEB UI. It is 443 by default.

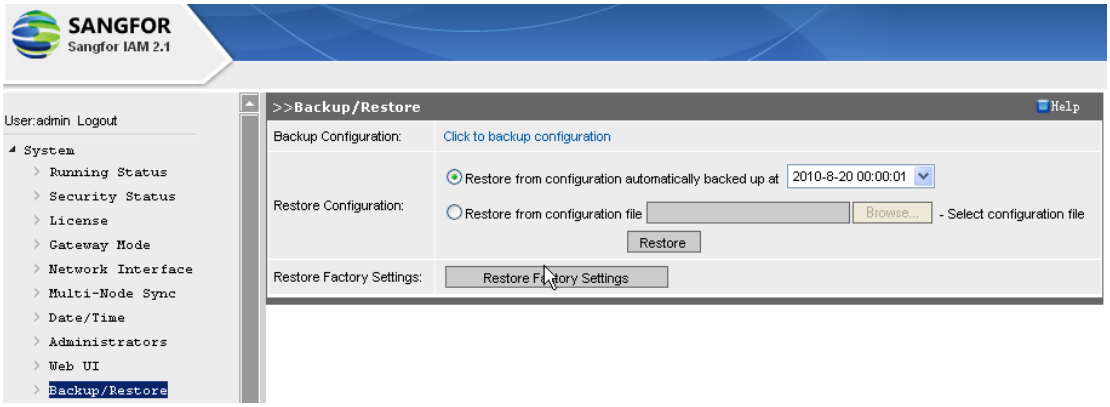
[Webpage Timeout]: If there is no operation on the console during this time interval, the console user will automatically log out the console.

[Operation Timeout]: If a page fails to open during this time interval, the system will think it times out and will not try to open this page again.

[Issue Console SSL Certificated To]: Configures the IP or domain name to which the SSL certificate of logging in to the console is issued.

[Download Console Root Certificate]: Click the link to download the SSL certificate of the console. Having the PC installed this certificate, the alarm prompt requesting for SSL certificate (when you are logging in to the console) will disappear.

3.10. Backup/Restore



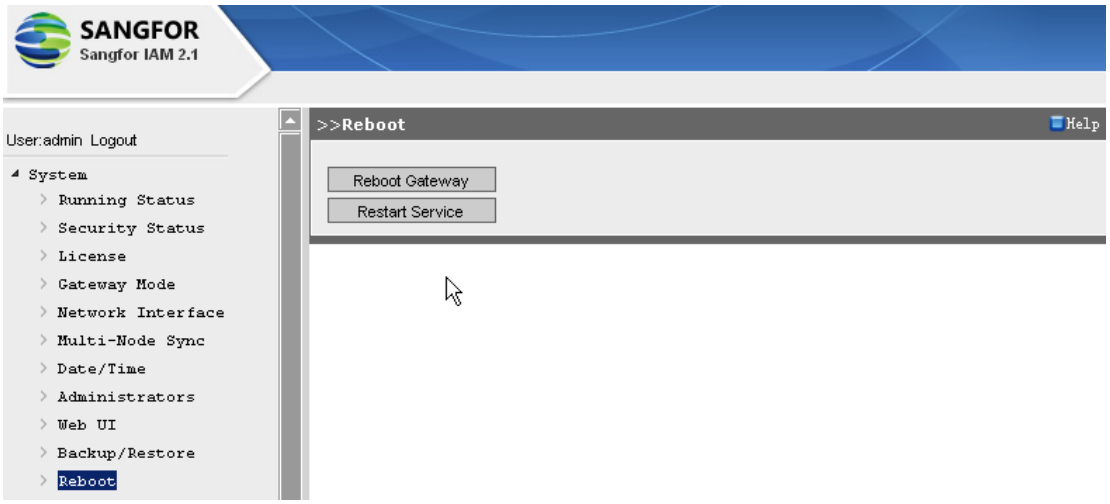
[Backup Configuration]: Click the link <Click to backup configuration> to download the configurations to the local computer and to backup them.

[Restore from configuration automatically backed up at some time]: Select the time when the configuration file is backed up. The backup configurations will replace the present ones. Generally, the configuration file will be backed up for 7 days.

[Restore from the configuration file]: Click the <Browse> button; select and upload a backed up configuration file, and then click the <Restore> button to have the backed up configuration replace the present one.

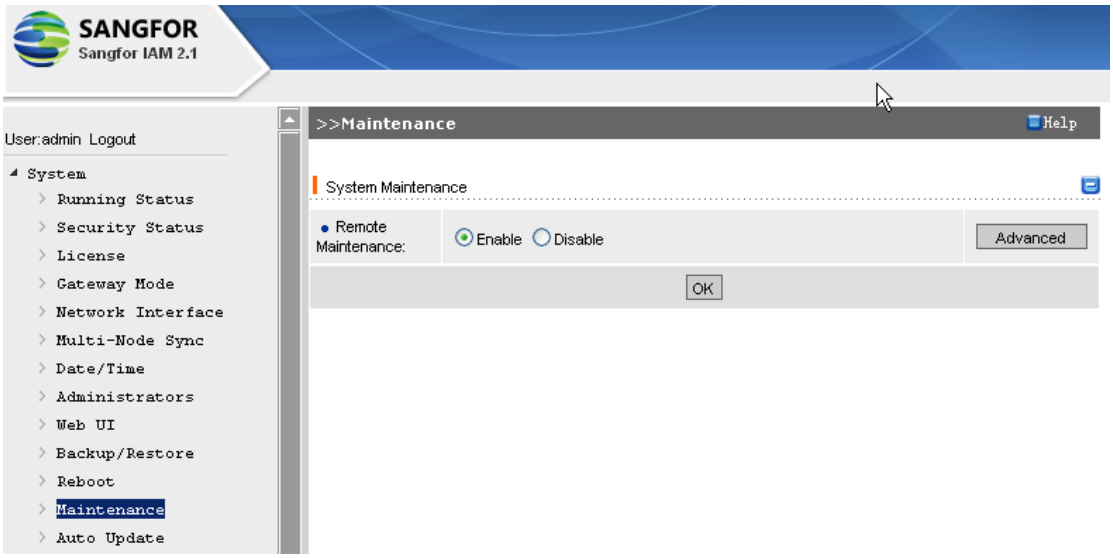
3.11. Reboot

You can [Reboot Gateway] or [Restart Service] on this page, as shown below:

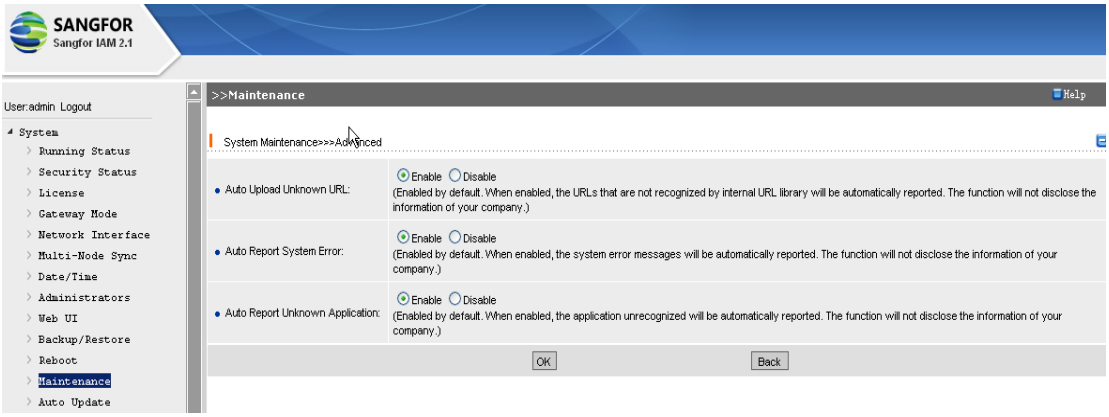


3.12. Maintenance

[Maintenance]: Defines whether to allow remote login through external network interface, whether to [Auto Upload Unknown URL], whether to [Auto Report System Error] and whether to [Auto Report Unknown Application].



Under the default configuration page, click the <Advanced> button to enter the [System Maintenance] > [Advanced] page and configure [Auto Upload Unknown URL], [Auto Report System Error] and [Auto Report Unknown Application], as shown below:



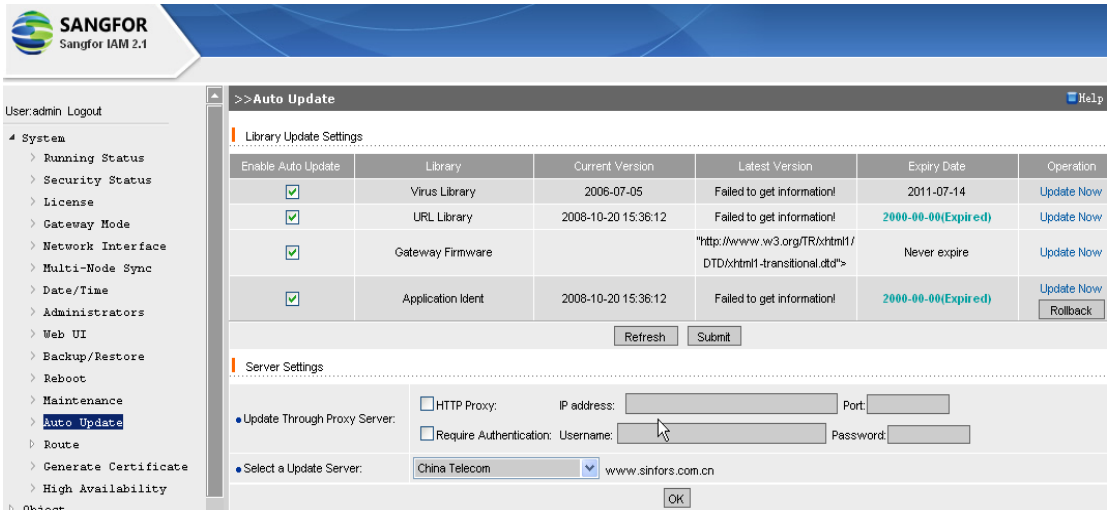
[Auto Upload Unknown URL]: Select [Enable] and the unknown URL found during using the IAM gateway device will be automatically uploaded.

[Auto Report System Error]: Select [Enable] and the anomaly information found during using the IAM gateway device will be automatically uploaded.

[Auto Report Unknown Application]: Select [Enable] and the unknown application information found during using the IAM gateway device will be uploaded.

3.13. Auto Update

[Auto Update]: Configure the update options of internal [Virus Library], [URL Library], [Gateway Firmware], [Application Ident], [Ingress Rule]. The configuration page is as shown below:



[Enable Auto Update]: Check the corresponding item to automatically update the internal library.

<Update Now>: Click this button to immediately update the corresponding library that has not been expired.

<Rollback>: Click this button to cancel the previous update of the corresponding library, and the rules library will recover to the previous version of library.

To update the library, the IAM gateway device should be ensured to connect to the Internet. If the IAM gateway device cannot access the Internet, you then need to configure [HTTP Proxy] options in [Server Settings] (provided there is HTTP proxy), so as to ensure the IAM gateway device can access the Internet smoothly and update the corresponding rules.

[HTTP Proxy] requires server [IP address] and [Port]; [Require Authentication] requires [Username] and [Password].

To ensure update speed, select an update server. Generally, the update process will go more quickly if the ISP server of the update server is the same with that used by the IAM gateway device.

3.14. Route

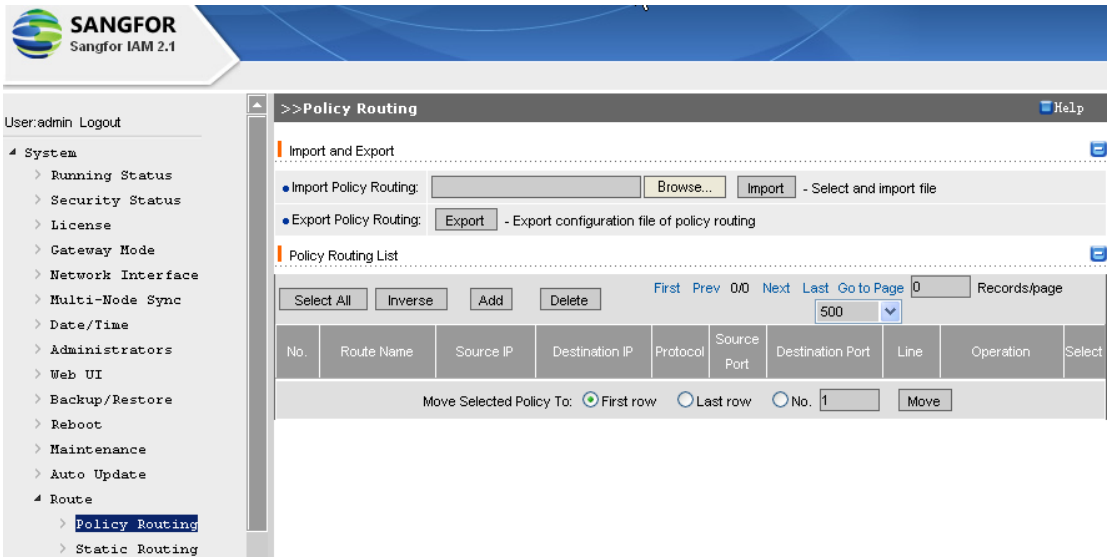
[Route] covers [Policy Routing] and [Static Routing], and mainly configures the route related to the IAM gateway device.

3.14.1. Policy Routing

SANGFOR IAM gateway device allows you to configure [Policy Routing]. Policy routing is

mainly used when IAM gateway connects to multiple external lines. Through configuring the source IP, destination IP, source port, destination port, protocol, etc., the policy-based route will be created. Therefore, which external line is the outgoing line to the external network is selected according to the manually-created policy.

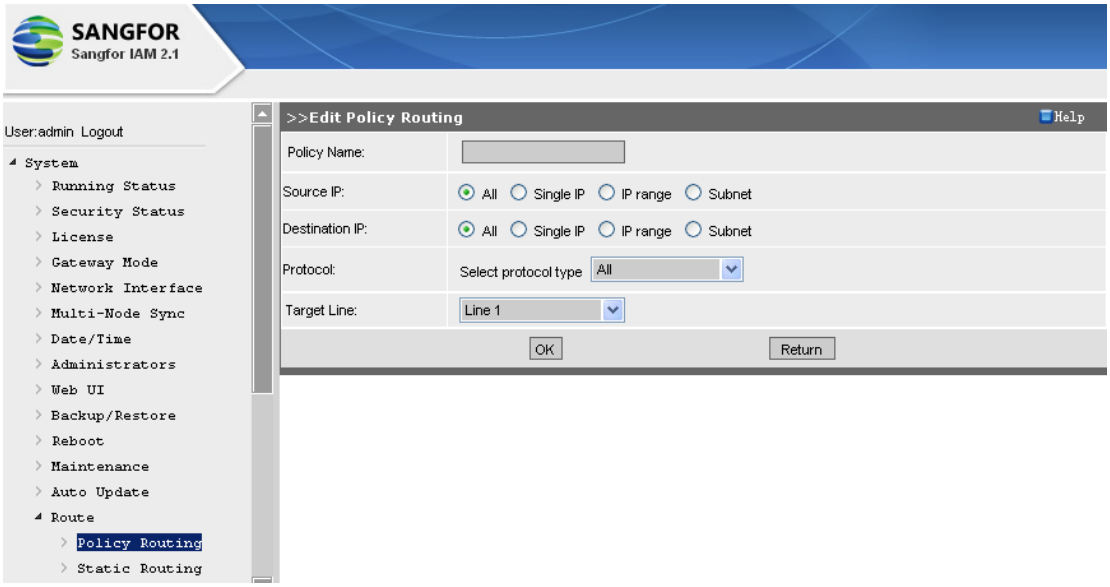
The [Policy Routing] configuration page is as shown below:



[Policy Routing List]: Displays the existing policy-based routings.

- If there are multiple applicable policy routings, the upper policy routing has higher priority to be matched.
- Click <UP> or <Down> to move up or move down the routing respectively; or [Select] an existing policy routing, and then select [First row] or [Last row] or [No.] to move this rule to top or bottom or to a specified row.

Click the <Add> button to enter the [Edit Policy Routing] page, as shown below:



[Policy Name]: Type in a unique name for this policy-based routing to distinguish it from others.

[Source IP], [Destination IP]: Configures the source IP, destination IP of the data packet on which this policy routing applies. Four options are available, namely, [All], [Single IP], [IP range] and [Subnet].

[Protocol]: Select a protocol for data packet transmission, [All] protocol, [TCP], [UDP], [ICMP] or [Others]. As to [TCP] and [UDP] protocol, you have to configure [Source Port] and [Destination Port]; for [Others] option, you have to enter [Protocol Number].

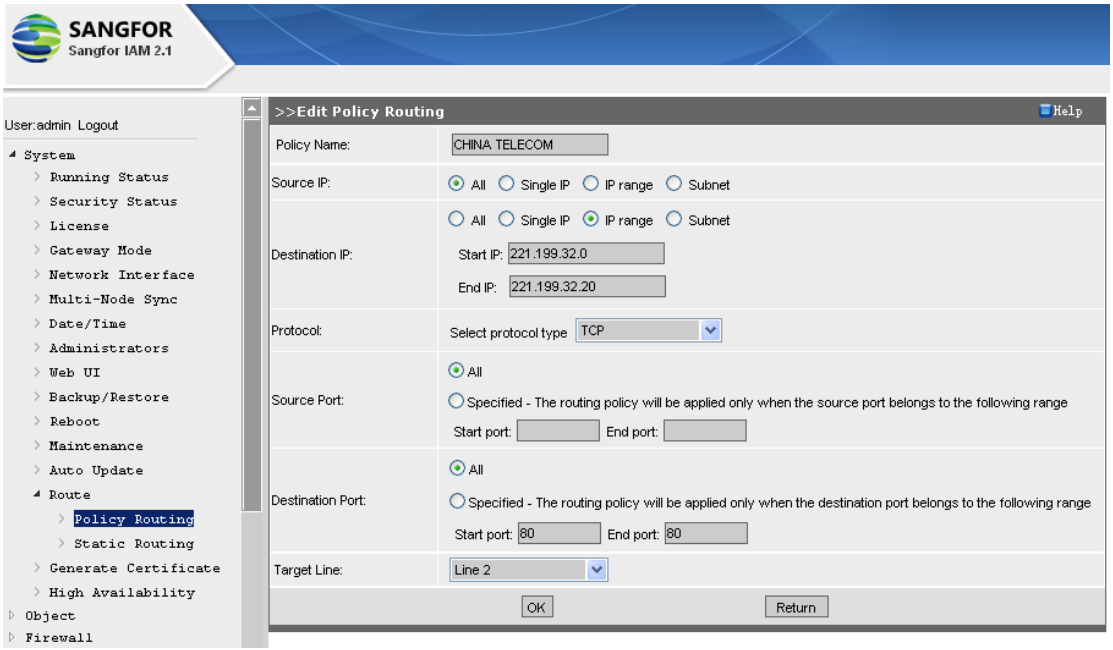
[Source Port], [Destination Port]: Configures the source port and destination port of the data packet on which this policy-based routing is applied.

[Target Line]: This target line is the outgoing line of the data packet if all the conditions configured above are matched.

Configuration Example of Policy Routing

Provided the IAM gateway device has two external lines. Line 1 is of CHINA NETCOM, Line 2 is of CHINA TELECOM. IP range of CHINA TELECOM is 221.199.32.0/20. We design a routing based on [Destination IP] 221.199.32.0/20, [Destination Port] 80, all the data packet passing through the [Target Line] Line 2.

To achieve traffic control of Internet access, we need to configure a policy routing rule. Specific steps and settings are as shown below:

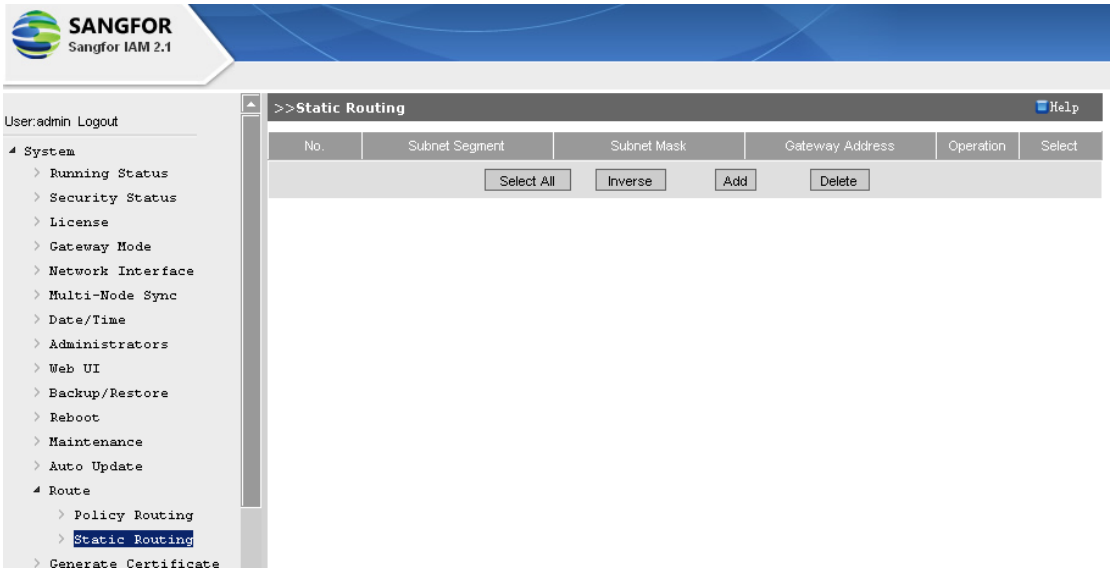


- If the selected [Target Line] is unavailable, IAM gateway device will arrange the data packets with an available target line.
- If you need the routing table of each ISP, please contact the Customer Service of SANGFOR. Having gained the routing table, click the <Browse> button to upload the policy routing and then click the <Import> button to import it.

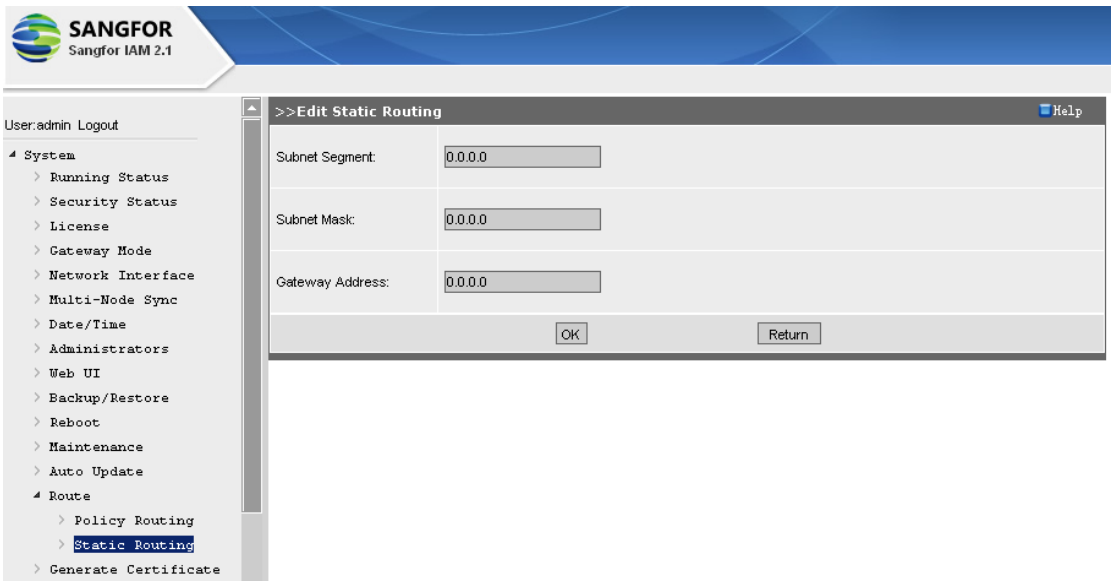
3.14.2. Static Routing

SAGFOR IAM gateway device allows you to configure [Static Routing].

The configuration page is as shown below:



Click the <Add> button and the [Edit Static Routing] configuration page appears:



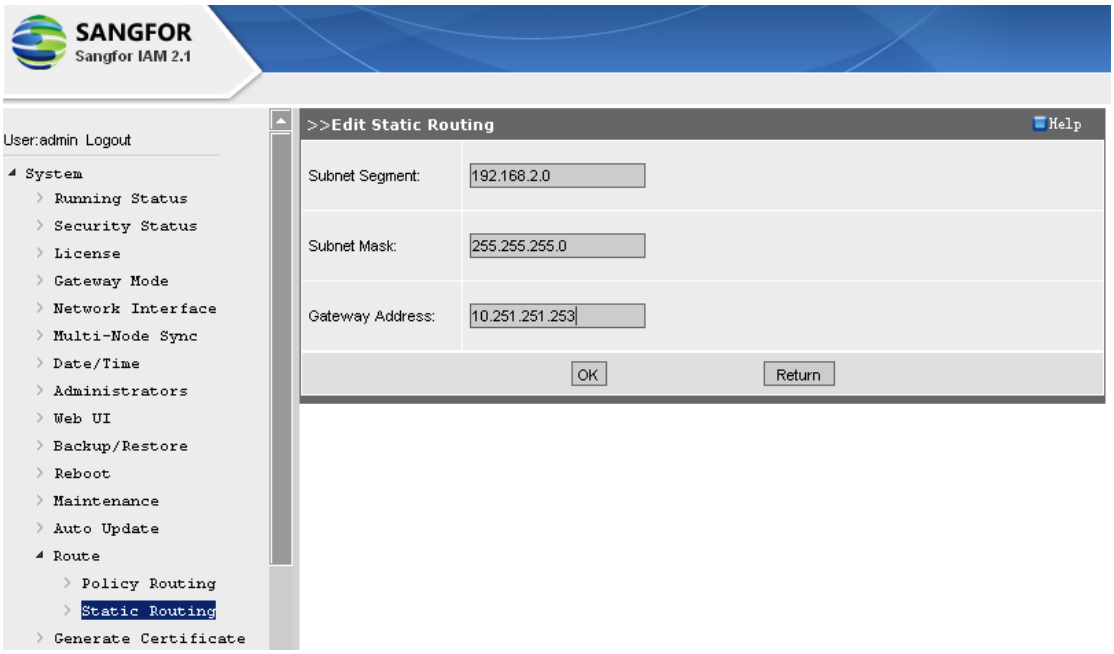
- [Static Routing] can enable the SNAT function (for multiple segments) to add return route.
- Add return route for SNAT function (for multiple segments)
- If there are several LAN segments access Internet through the SANGFOR gateway device, then you need to add a [Static Routing], so that the IAM gateway device can return the data packets of the LAN users (of different segments) to the LAN switch/route device properly.

Configuration Example of Static Routing

Provided that, there are two LAN segments, 10.251.251.X and 192.168.2.X, which are connected to each other through a layer 3 switch. The LAN PCs of both the segments direct to the corresponding gateway configured on the layer 3 switch. The LAN interface IP of the IAM gateway device is 10.251.251.251 (of 10.251.251.X segment). The WAN interface connects to the public network.

Requirement: Users of 10.251.251.X and 192.168.2.X segments get access to the Internet through IAM gateway device, IAM gateway device acting as the egress.

Since 192.168.2.X and the LAN interface (10.251.251.251) of IAM gateway device are of different segments, IAM gateway device has to add a static routing, the data packets from 192.168.2.X being forwarded to and handled by the LAN layer 3 switch (10.251.251.253) and finally back to the PC(s) of 192.168.2.X segment. Specific steps and configurations are as shown below:



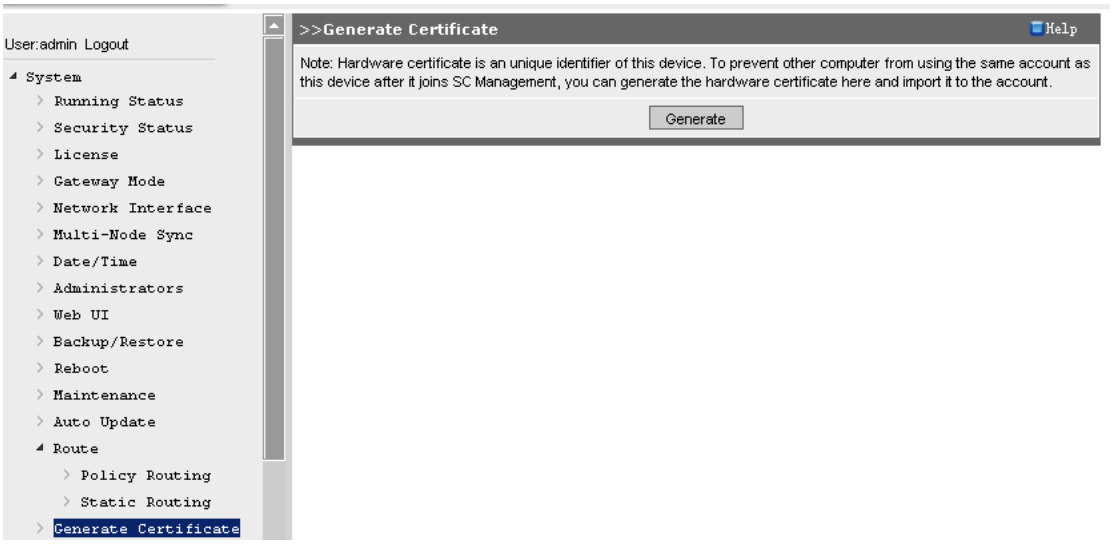
Add the SNAT segments, namely, 10.251.251.0/24 and 192.168.2.0/24. For detailed steps, please refer to Section 6.2.1 System Settings.

Add a static route in [Static Routing] page, the LAN IP addresses 192.168.2.0/24 directing to gateway 10.251.251.253.

3.15. Generate Certificate

[Generate Certificate]: Generates the hardware certificate which is the only label to distinguish this device. This certificate can function as its ID when it registers on the SC (Secure Center) Management.

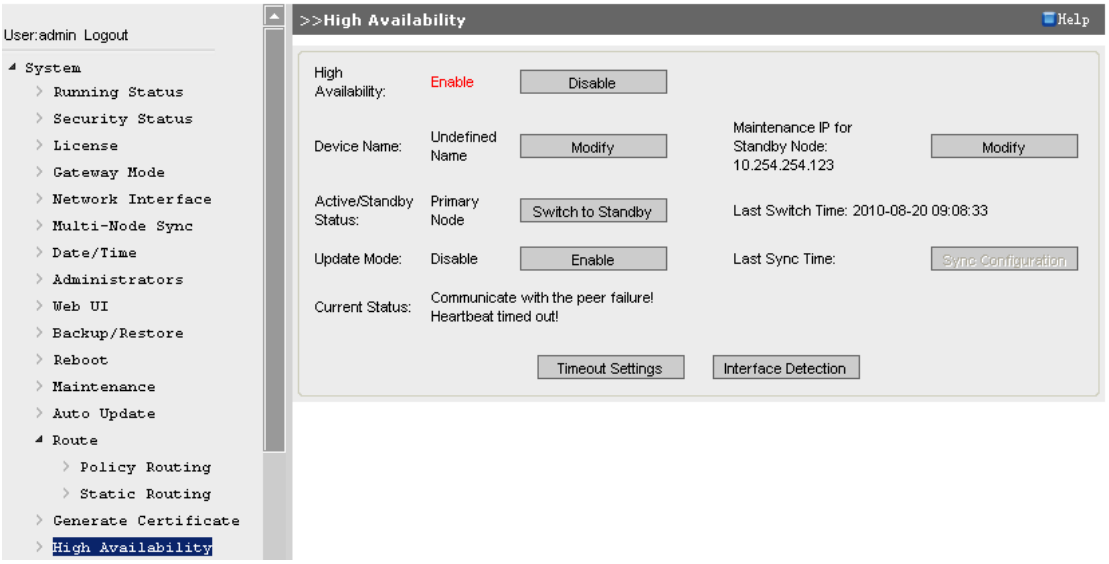
The [Generate Certificate] page is as shown below:



3.16. High Availability

[High Availability] configured the mode of the redundant system (high availability). Setting options are [High Availability], [Device Name], [Active/Standby Status], [Update Mode], [Current Status].

The configuration page is as shown below:

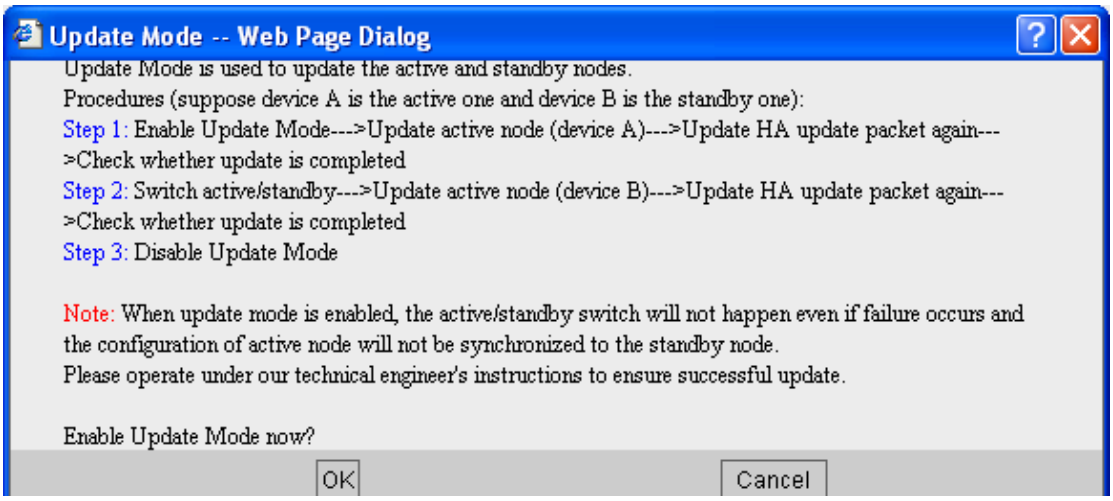


[High Availability]: Displays the status of this function, enabled or disabled.

[Device Name]: Displays the name the local device. Click <Modify> to edit the device name.

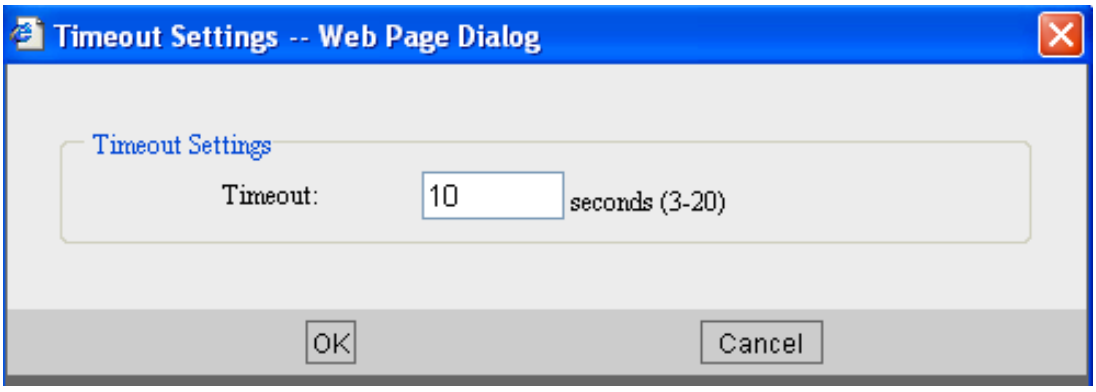
[Active/Standby Status]: Displays the active or standby status of the local device. Click the <Switch to Active> or the <Switch to Standby> button to switch the standby node to Active or switch the active node to Standby.

[Update Mode]: Click this button to update the primary node, and lock the Active/Standby status. Click [Enable] and the Active/Standby status cannot be altered, even though the primary node is down. Please think it over to enable this function. It is recommended to enable [Update Mode] when you are to update the primary and standby device; completing update, please disable [Update Mode]. Click <Enable> and the following dialog pops up:


Update Mode -- Web Page Dialog
Update Mode is used to update the active and standby nodes.
Procedures (suppose device A is the active one and device B is the standby one):
Step 1: Enable Update Mode--->Update active node (device A)--->Update HA update packet again--->Check whether update is completed
Step 2: Switch active/standby--->Update active node (device B)--->Update HA update packet again--->Check whether update is completed
Step 3: Disable Update Mode
Note: When update mode is enabled, the active/standby switch will not happen even if failure occurs and the configuration of active node will not be synchronized to the standby node.
Please operate under our technical engineer's instructions to ensure successful update.
Enable Update Mode now?
OK
Cancel

[Current Status]: Displays the communication status between primary and standby device, and the timeout information as well. Timeout can be user-defined.

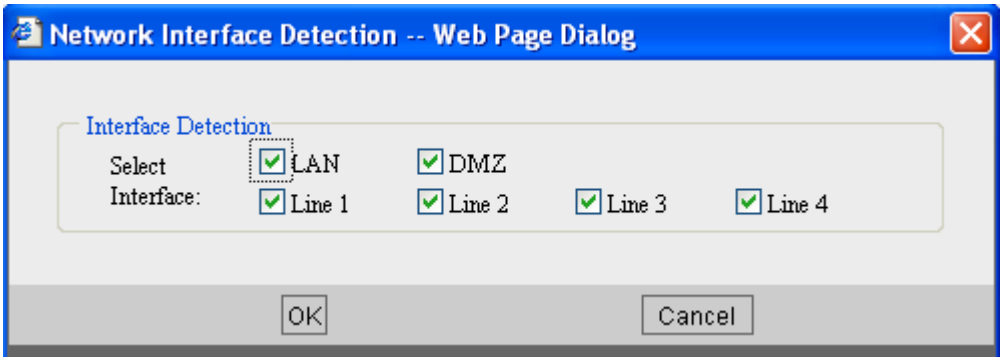
<Timeout Settings>: Click this button to enter the [Timeout Settings] page and define the communication detection timeout, as shown in the following figure:



Configuration Example of High Availability

Timeout of the primary node is 10 seconds, the primary node will send message to the standby node every 10 seconds. If the standby node does not receive the message from the primary node in 10 seconds, the standby node will think the primary node got down and switch from Standby status to Active status automatically.

Click the <Interface Detection> button to enter the [Network Interface Detection] dialog and select the network interface(s) of the host to be detected. If any of the selected network interfaces is down, the standby node switches to Active status. The interface can be any of the device interfaces that connect to the public network. The configuration page is as shown below:



Chapter 4 Object

[Object] covers configuration of [Application Ident Rule], [Intelligent Ident Rule], [Server], [IP Group], [Schedule], [URL Group], [White List Group], [Keyword Group], [File Type Group], [Ingress Rule] and [SSL Certificate].

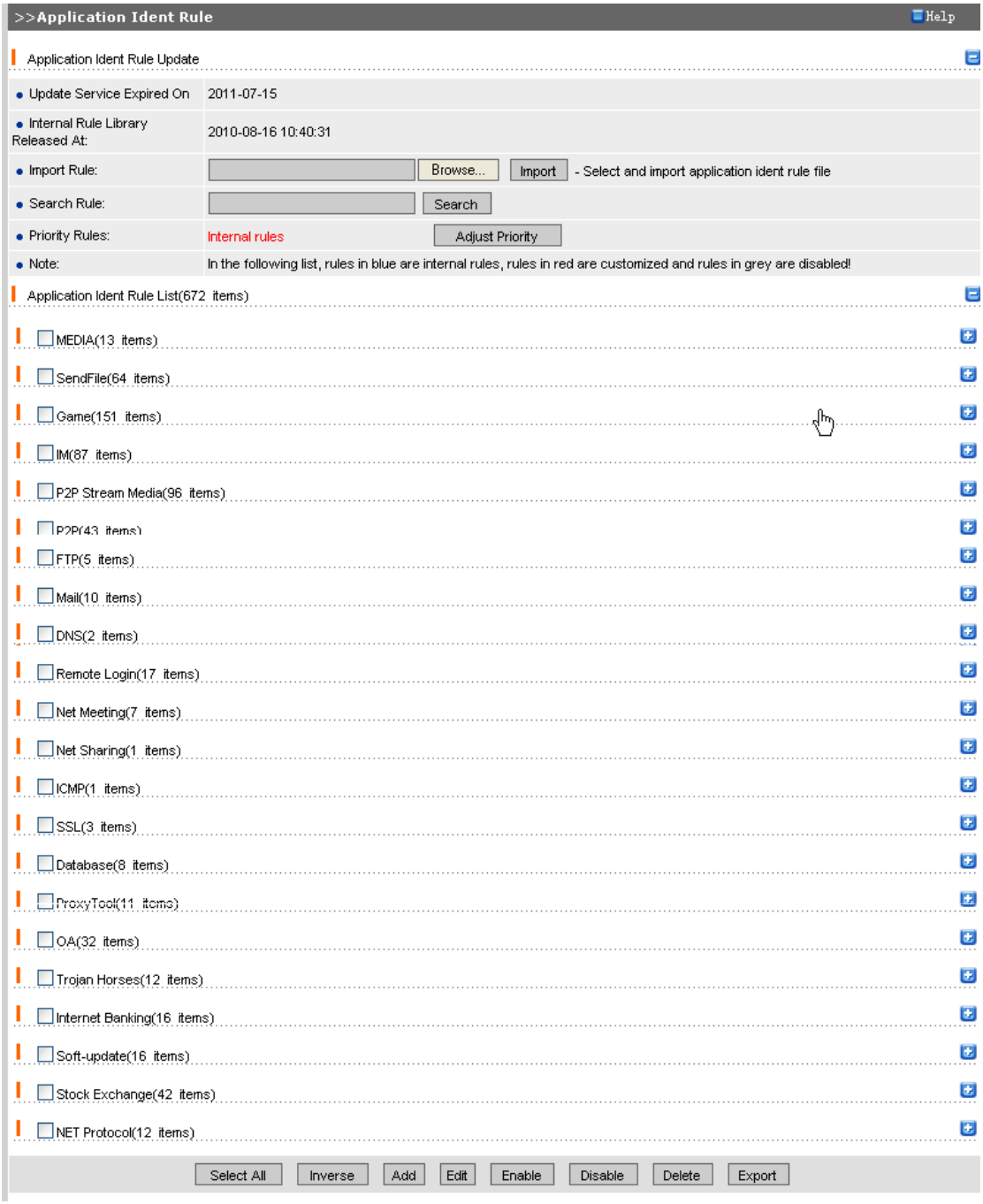
4.1. Application Ident Rule

Download software such as BT, emule, etc., consumes lots of bandwidth resource; IM software such as QQ, MSN and stock trading software, etc., definitely occupies the office hours and lowers down working efficiency. Though most of the enterprises issue regulations to ban their staff from using these software tools, however, they can do nothing to prevent their staff from using them, for nearly all of these software tools are designed to be able to shy away from the general firewalls.

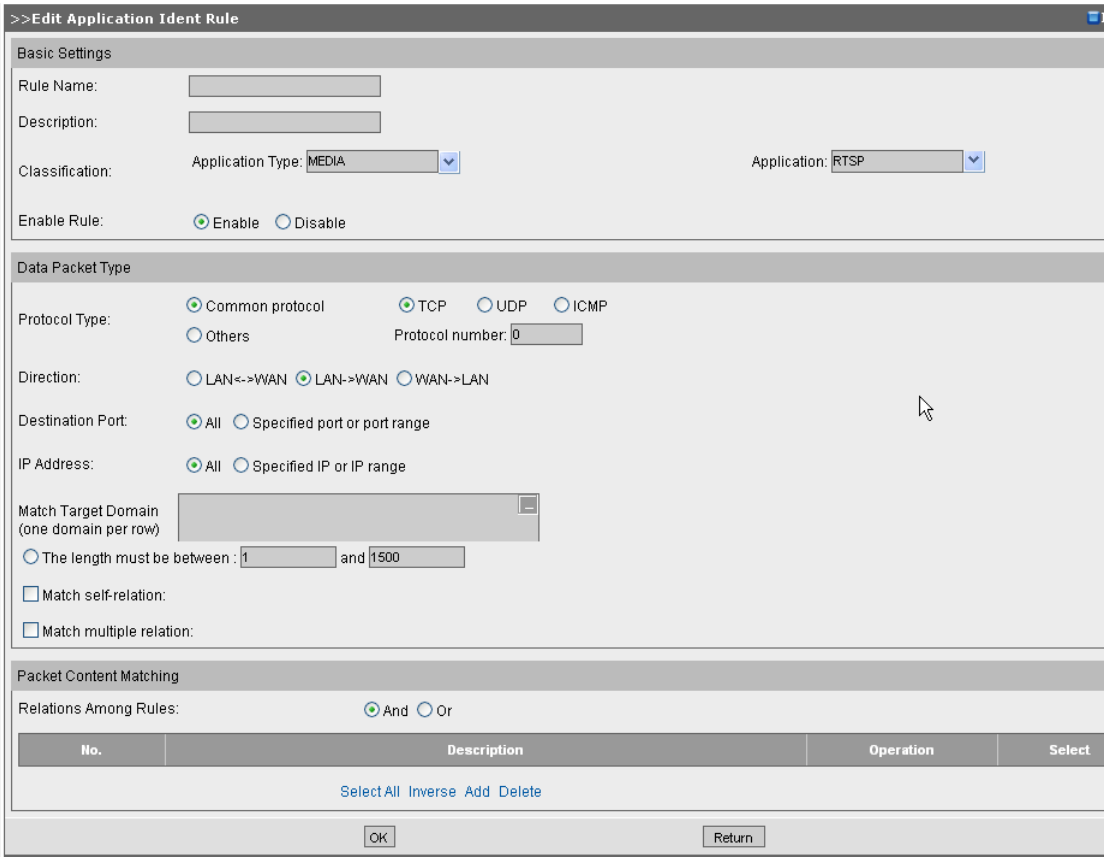
Application identification rule can detect traffic on the basis of protocol, port, direction, length of data packet, and the content of the data packets, etc., which helps to identify P2P traffic quite well. Application identification rule falls into internal rule and user-defined rule. The internal rules cannot be modified, while the user-defined rule can be added, deleted, and edited, etc.

To obtain flow information of specific applications, you can choose the corresponding application type or application, in association with the [Service Control] configuration in [IAM] > [Access Control Policy] page > [Access Control], and [Bandwidth Settings] configuration in [Bandwidth Management], to create a policy.

SANGFOR IAM gateway device adopts some patented technology to efficiently block the above mentioned chat and IM software tools. Because the data packets of each kind of software have a unique feature value, when the software communicates with the external networks, IAM gateway device will detect the feature contained in the data packets and determines whether the data packets should be blocked. If the data packets contain the features we configured, then it will not be sent or received. In this way, this software will be unavailable for the LAN users.



The key to identify the application is to analyze the features of these data packets. SANGFOR will periodically provide the feature values definition of the software such as P2P, IM, etc. You can contact SANGFOR and apply for application identification rule packets to manually import the rules, and you can analyze data packets by yourself and define your own application identification rule by clicking the <Add> button. The pop-up [Edit Application Ident Rule] configuration page is as shown below:



Configure in [Packet Content Matching] section the feature value according to the analysis on the data packets.

[Internal Rule Library Released At]: Indicates the latest time that the current version of internal rule library was released at.

[Application Ident Rule] supports [Import] and [Export] of the rules. To export the existing user-defined rule(s), just check the rule(s), click the <Export> button and name the file, and then finally confirm to export (the internal rule cannot be exported).

[Import Rule]: To import a rule, click the <Browse> button and upload the rule (extension of the rule file is *.ccf), then click the <Import> button.

[Search Rule]: Type in the keyword of a rule name, click the <Search> button and you can find the rule whose name contains this keyword.

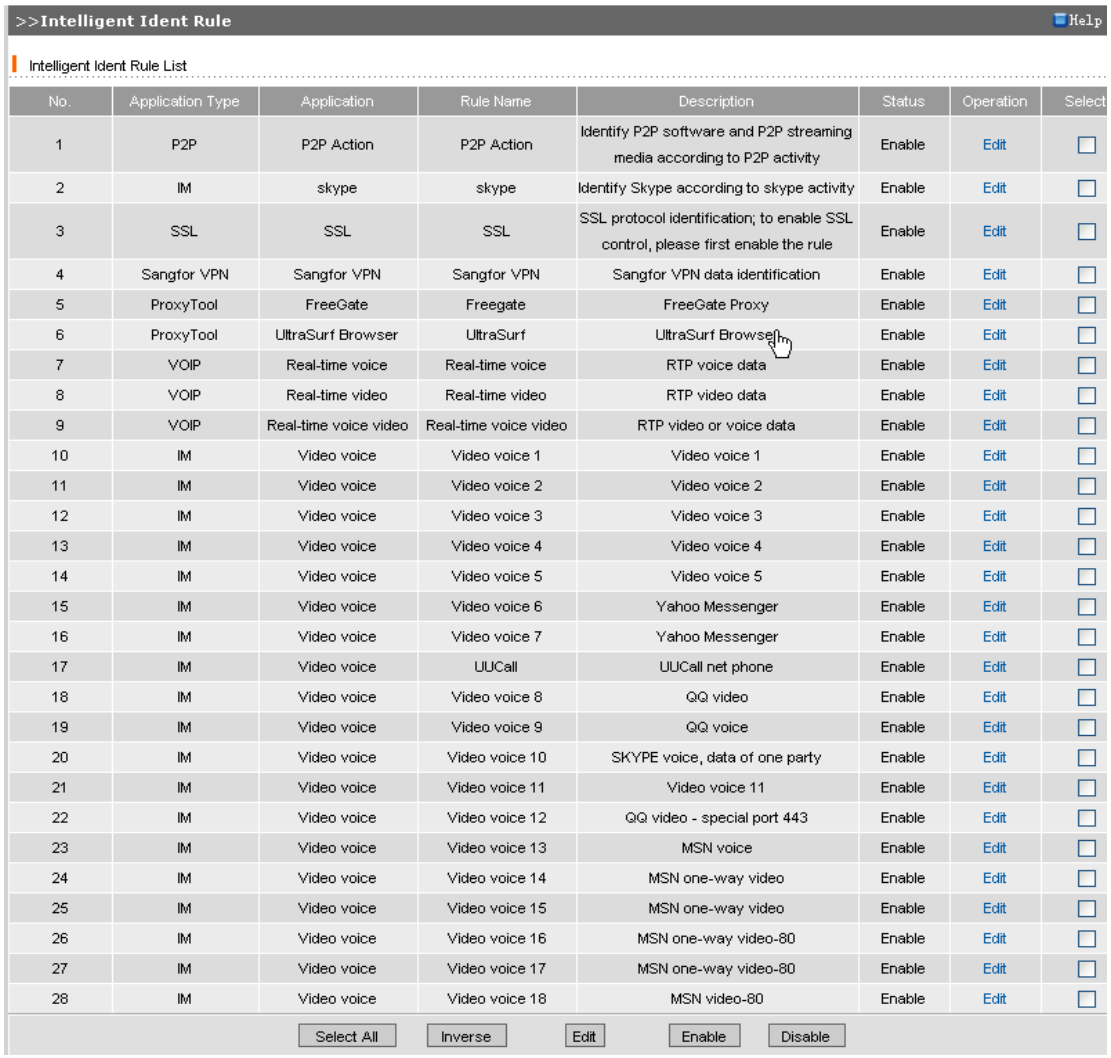
[Priority Rules]: Click the <Adjust Priority> button to switch the priority between the user-defined application identification rules and the internal rules. The type of rules that has higher priority to be matched is displayed in red.

- Since BT and IM software differ from each other and keep updating, some application identification rules may get invalid for some versions of the software. SANGFOR will periodically update the application identification rules. Please make sure your IAM gateway device can access the Internet.
- For the internal rules, you can only alter the classification, but not edit the policy or export the rule.

4.2. Intelligent Ident Rule

[Intelligent Ident Rule] mainly identifies the plain text or cipher text form P2P applications, identifies the encrypted Skype data according to the Skype actions, and identifies the SSL certificate, SANGFOR VPN data, data from proxy tool, and the VOIP and IM video and voice data.

The configuration page is as shown below:



>>Intelligent Ident Rule — Help

Intelligent Ident Rule List

No.	Application Type	Application	Rule Name	Description	Status	Operation	Select
1	P2P	P2P Action	P2P Action	Identify P2P software and P2P streaming media according to P2P activity	Enable	Edit	
2	IM	skype	skype	Identify Skype according to skype activity	Enable	Edit	
3	SSL	SSL	SSL	SSL protocol identification; to enable SSL control, please first enable the rule	Enable	Edit	
4	Sangfor VPN	Sangfor VPN	Sangfor VPN	Sangfor VPN data identification	Enable	Edit	
5	ProxyTool	FreeGate	Freegate	FreeGate Proxy	Enable	Edit	
6	ProxyTool	UltraSurf Browser	UltraSurf	UltraSurf Browser	Enable	Edit	
7	VOIP	Real-time voice	Real-time voice	RTP voice data	Enable	Edit	
8	VOIP	Real-time video	Real-time video	RTP video data	Enable	Edit	
9	VOIP	Real-time voice video	Real-time voice video	RTP video or voice data	Enable	Edit	
10	IM	Video voice	Video voice 1	Video voice 1	Enable	Edit	
11	IM	Video voice	Video voice 2	Video voice 2	Enable	Edit	
12	IM	Video voice	Video voice 3	Video voice 3	Enable	Edit	
13	IM	Video voice	Video voice 4	Video voice 4	Enable	Edit	
14	IM	Video voice	Video voice 5	Video voice 5	Enable	Edit	
15	IM	Video voice	Video voice 6	Yahoo Messenger	Enable	Edit	
16	IM	Video voice	Video voice 7	Yahoo Messenger	Enable	Edit	
17	IM	Video voice	UUCall	UUCall net phone	Enable	Edit	
18	IM	Video voice	Video voice 8	QQ video	Enable	Edit	
19	IM	Video voice	Video voice 9	QQ voice	Enable	Edit	
20	IM	Video voice	Video voice 10	SKYPE voice, data of one party	Enable	Edit	
21	IM	Video voice	Video voice 11	Video voice 11	Enable	Edit	
22	IM	Video voice	Video voice 12	QQ video - special port 443	Enable	Edit	
23	IM	Video voice	Video voice 13	MSN voice	Enable	Edit	
24	IM	Video voice	Video voice 14	MSN one-way video	Enable	Edit	
25	IM	Video voice	Video voice 15	MSN one-way video	Enable	Edit	
26	IM	Video voice	Video voice 16	MSN one-way video-80	Enable	Edit	
27	IM	Video voice	Video voice 17	MSN one-way video-80	Enable	Edit	
28	IM	Video voice	Video voice 18	MSN video-80	Enable	Edit	

Select All | Inverse | Edit | Enable | Disable

- [Application Ident Rule] detects the P2P application as well, limited to plaintext P2P data. If you disable the [P2P Action] (in the Intelligent Ident Rule List on the [Intelligent Ident Rule] page), it can still successfully identify the plaintext P2P data but fails to identify the cipher text P2P data.
- Skype data are encrypted. To control and record the Skype data, you have to configure it on the [Edit Intelligent Ident Rule] page of [P2P Action], put in another way, you have to first enable [P2P Action] (in the [Intelligent Ident Rule List] on the [Intelligent Ident Rule] page), and then select the Skype application and enable the rule on the [Edit Intelligent Ident Rule] page of [P2P Action].
- As to control and record of video voice applications such as IM, VOIP, etc., you have to configure and enable the [VOIP] rule in [Intelligent Ident Rule] > IM [Edit Intelligent Ident

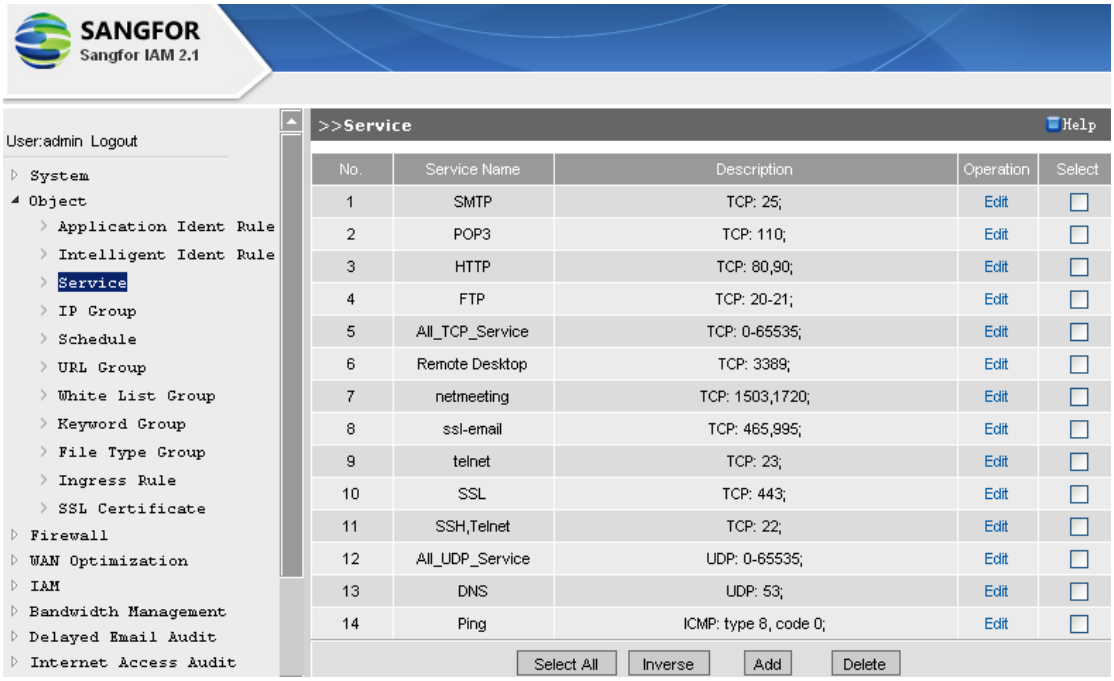
Rule] and [Intelligent Ident Rule] > VOIP [Edit Intelligent Ident Rule].

4.3. Service

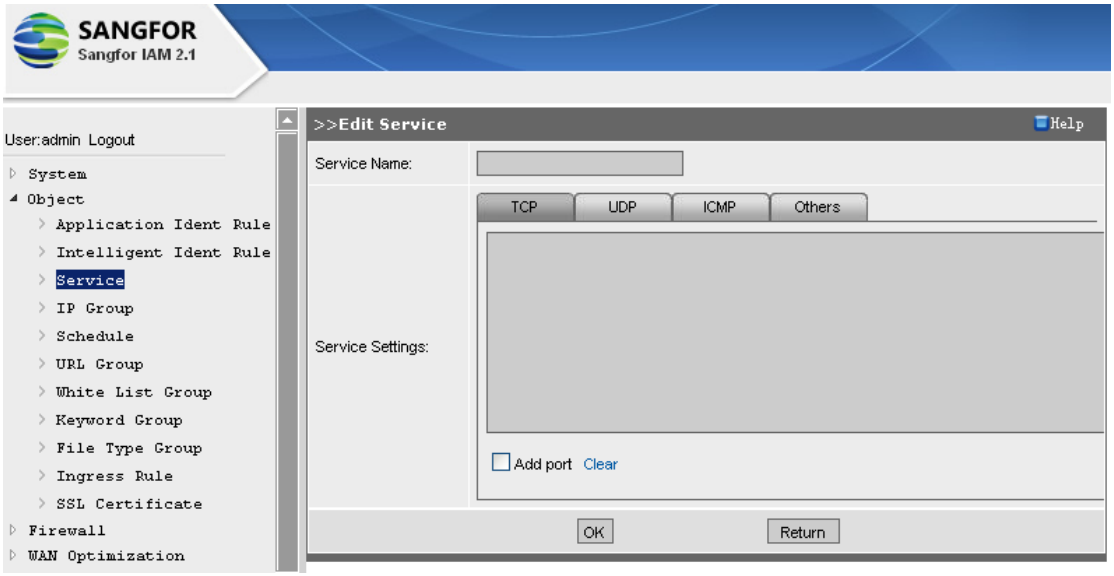
[Service] generally is in association with the rule configured in [Firewall] > [Firewall Rules] and rules configured in [IAM] > [Access Control Policy] page > [Access Control] > [Service Control].

First, you need to define various services of the firewall in [Object] > [Service] including the port and protocol applied; next, configure the filtering rules in [Firewall] > [Firewall Rules], referring to the services defined previously, or configure access control in [IAM] > [Access Control Policy] page > [Access Control] > [Service Control] according to the services defined previously.

The configuration is as shown below:

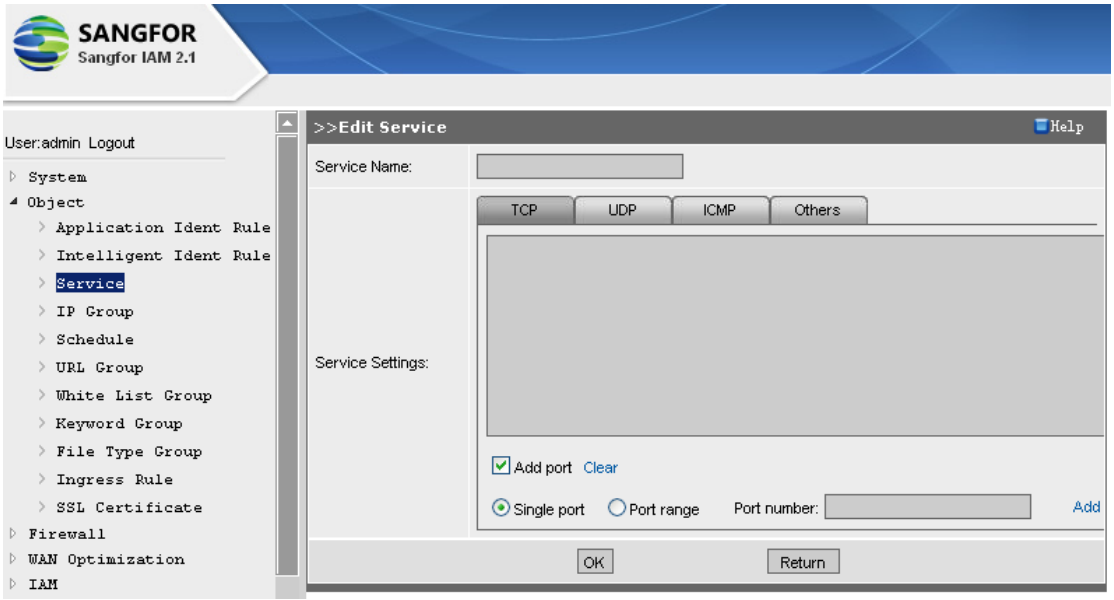


Click the <Add> button, and the [Edit Service] page pops up, as shown below:



[Service Name]: Type in a unique name for this new service (the characters better be easy for memory) to distinguish it from others.

Click [TCP], [UDP], [ICMP] or [Others] to define the protocol to be applied; check [Add Port] and type in a single port or a port range, as shown below:

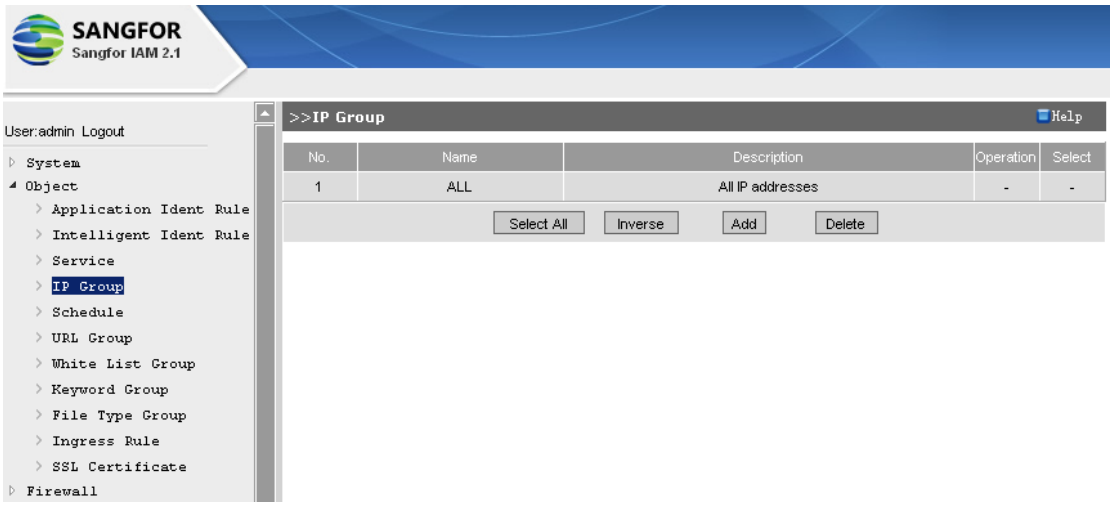


If it is [Other] protocol, [Protocol number] 0 indicates all the protocols.

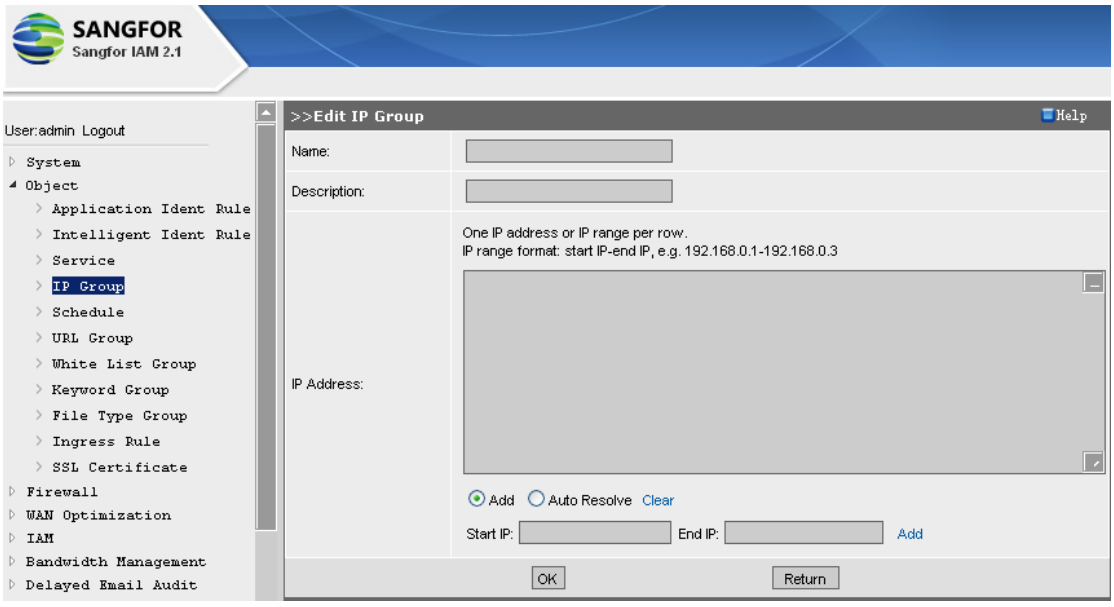
4.4. IP Group

An [IP Group] consists of some IP addresses which may be LAN IP range or WAN IP range or all the IP addresses.

[IP Group] generally is in association with the rule configured in [Firewall] > [Firewall Rules]. It configures the source IP address, destination IP addresses, or defines the LAN users in association with [IAM] > [Organization Structure] page > [Edit User] > [User Attribute] > [Binding] > [Bind IP] > [Get from IP group], or defines the destination IP group in [IAM] > [Access Control Policy] page > [Access Control] > [Service Control].



Click the <Add> button and the following [Edit IP Group] page pops up, as shown below:

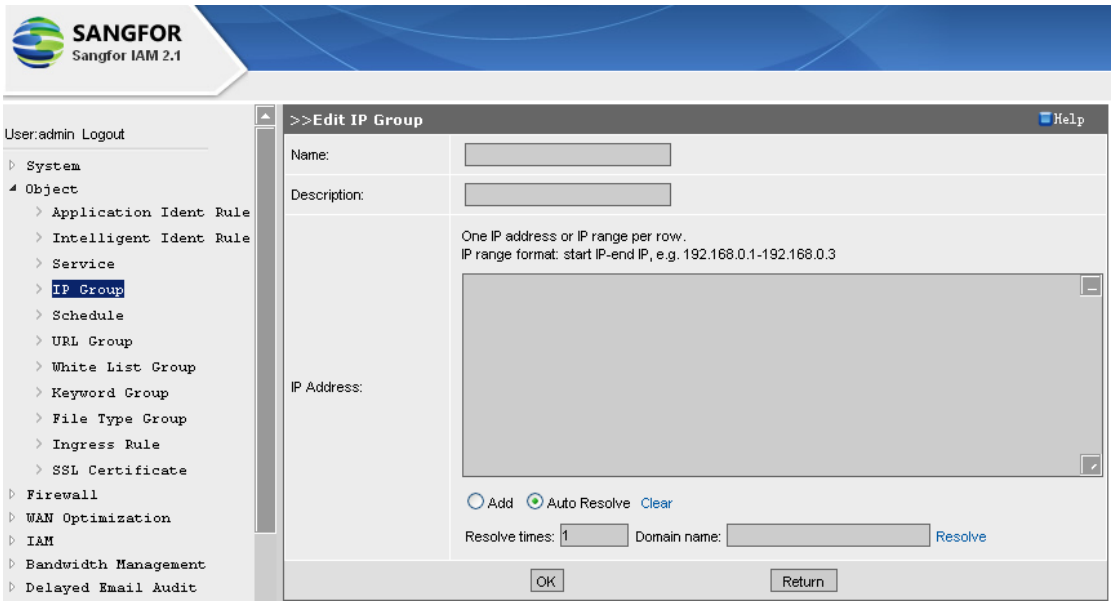


[Name]: Names the newly-created IP group.

[Description]: Type in a brief description for this IP group.

[IP Address]: Defines the IP addresses contained by the IP group. Select [Add] and type in the [Start IP] and [End IP] and then click the <Add> to add the IP address into the list; or select [Auto Resole], type in the domain name and click <Resolve> to have the resolved IP addresses listed.

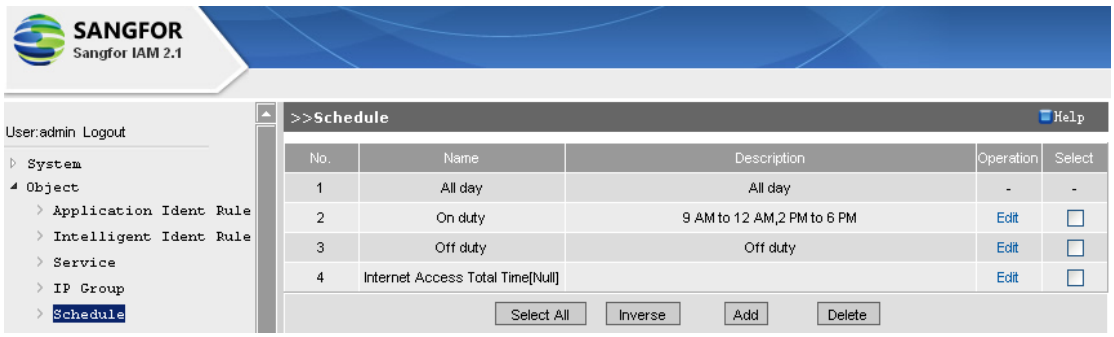
Finally, you have to click the <OK> button to save all the settings.



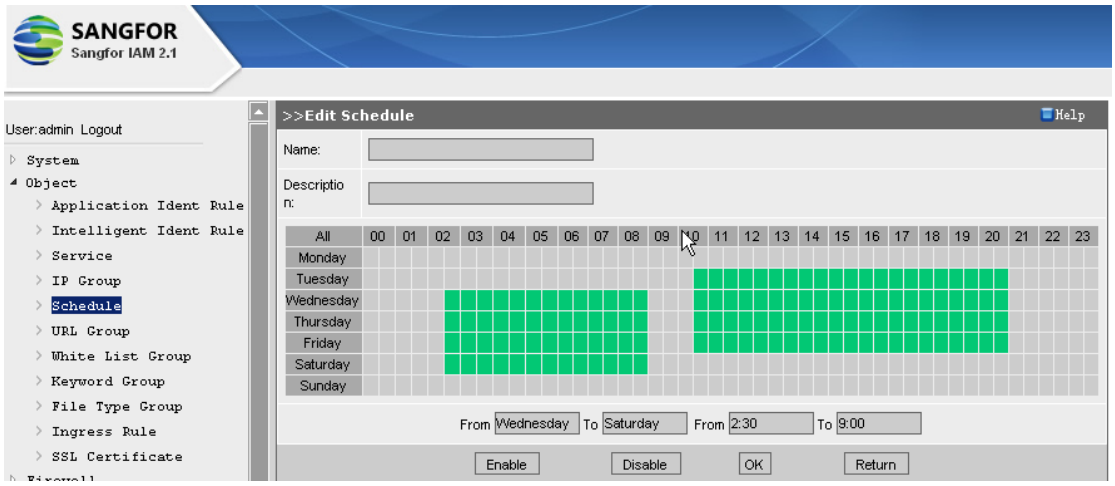
The local PC can [Auto Resolve] the domain name, with the condition that the Internet is accessible to it.

4.5. Schedule

[Schedule] defines the commonly used time periods, mainly used as valid time or expiry time. The defined schedule can be referenced by [Firewall] > [Firewall Rules], and [IAM] > [Access Control Policy] > [Access Control], and [Bandwidth Management] > [Bandwidth Settings] configuration pages.



Click the <Add> button to enter the [Schedule] configuration page, as shown below:



[Name]: Names the newly-created schedule.

[Description]: Type in a brief description for this schedule.

Click (or click and drag) the needed time periods in the table and click the <Enable> button to enable the selected time periods; and then click the <OK> button to save the settings on this page.

4.6. URL Group

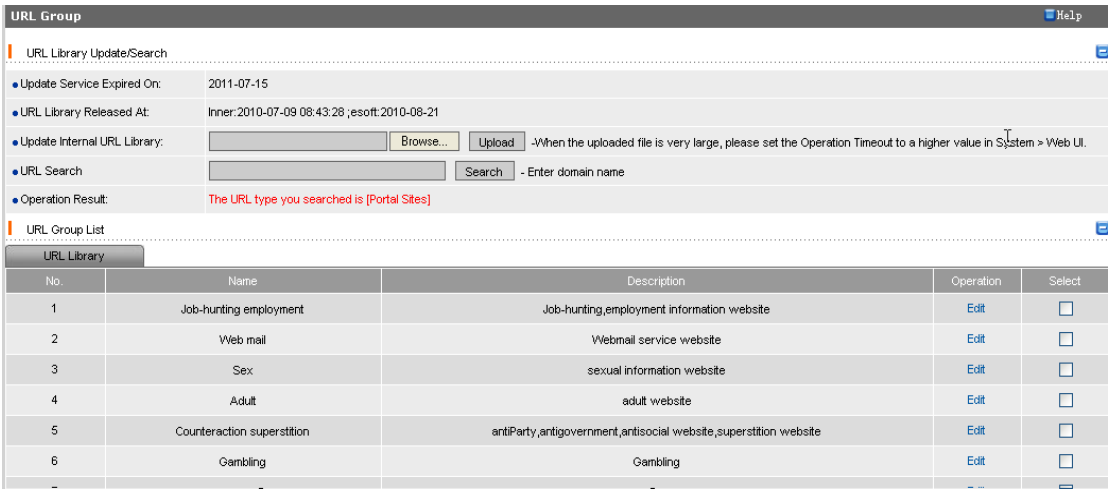
[URL Group] is created according to the URL library, and can be referenced by [URL Filter] configuration in [IAM] > [Access Control Policy] > [Web Filter] > [HTTP URL Filter] and [HTTPS URL Filter], and by [Bandwidth Channel] configuration in [Bandwidth Management] > [Bandwidth Settings] page, to achieve URL access filtering and bandwidth control.

URL Group
Help
URL Library Update/Search
Update Service Expired On: 2011-07-15
URL Library Released At: Inner:2010-07-09 08:43:28 ;esoft:2010-08-21
Update Internal URL Library: Browse... Upload -When the uploaded file is very large, please set the Operation Timeout to a higher value in System > Web UI.
URL Search Search - Enter domain name
URL Group List
URL Library
No. Name Description Operation Select
1 Job-hunting employment Job-hunting,employment information website Edit
2 Web mail Webmail service website Edit
3 Sex sexual information website Edit
4 Adult adult website Edit
5 Counteraction superstition antiParty,antigovernment,antisocial website,superstition website Edit
6 Gambling Gambling Edit
7 Online Payment Online payment website Edit
21 Education university website,education website Edit
22 Government organization government organization Edit
23 Realty decoration realty decoration website Edit
24 Life correlation health,shopping online,car,tourism Edit
25 Military military relative information website Edit
26 Literature literature website Edit
27 Religion Religion information website Edit
28 Pyramid-selling advertisement network pyramid-selling,advertisement website Edit
29 Virus fishing virus,network fishing website Edit
30 Youth children Youth children website Edit
31 Poison poison criminous website Edit
32 Violence & Immorality violence & immorality website Edit
33 Nonprofit Organization nonprofit Organization website Edit
34 Criminal skill educate criminal skill Edit
35 Law correlation law information website Edit
36 Network Harddisk Network Harddisk Edit
37 Movie music movie music website Edit
38 Online video Online video website Edit
39 Welfare Lottery The provision of welfare lottery information, on-line purchase of the website Edit
40 Web Proxy Web Proxy website Edit
41 Stock Quotes Including equities, the Fund's website message Edit
42 Compromised and Links to Malware Sites that have been compromised by someone other than the site owner Edit
43 Spyware and Malicious Sites Sites or software that installs on a user's computer to collect information without authoriz... Edit
44 Download Sites Shareware, freeware, and other legal software downloads Edit
45 Translator Translate sites from one language to another Edit
46 Alcohol Web pages that promote, advocate or sell alcohol including beer,wine and hard liquor Edit
47 Pharmaceuticals Prescribed medications and information about legal drugs, drug studies, etc Edit
48 Tobacco Sites that promote or sell tobacco products such as cigarettes, cigars, and chew Edit
49 Personal Webpages Sites about or hosted by personal individuals Edit
50 Humor Comedians, comic strips, jokes, and other humorous content or diversions Edit
51 Portal Sites General sites with customizable personal home pages, parked domains, and sites that co... Edit
52 Business/Services Any business, offers or service Edit
53 Spam URLs Web site links found inside spammed e-mails are automatically added to this list Edit
54 Miscellaneous Websites that do not have any content,contain blank or missing pages or that just do not ... Edit
Select All Inverse Add Delete

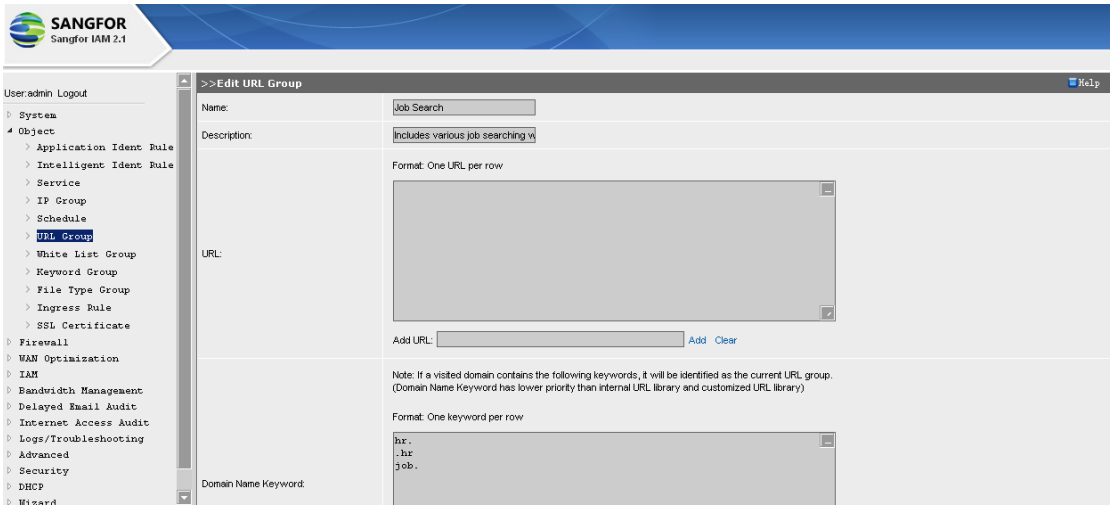
[URL Library Released At]: Indicates the latest time that the current version of URL library was released at.

[Update URL Library]: If the URL library cannot automatically update for it is disconnected to the Internet, you can manually update the URL library. Just click the <Browse> button and upload the URL library file from the local PC, and then click the <Upload> button.

[URL Search]: Enter the domain name into [URL Search] and click the <Search> button to search whether this domain name exists in the URL library and in which URL group this domain name is contained. For instance, type in *www.sina.com* and click the <Search> button, the search result is displayed, as shown in the following figure:



IAM gateway device is built in with a large number of URL groups when it is delivered from the factory. You can add a new URL into the URL library if necessary, in addition to using the existing and built-in URLs.



[Name]: Name the new URL group.

[Description]: Type in a brief description for this new URL group

[URL]: Type the domain name (URL) into the text box. The URL group consists of the URL(s) in this list. The wildcard character is supported.

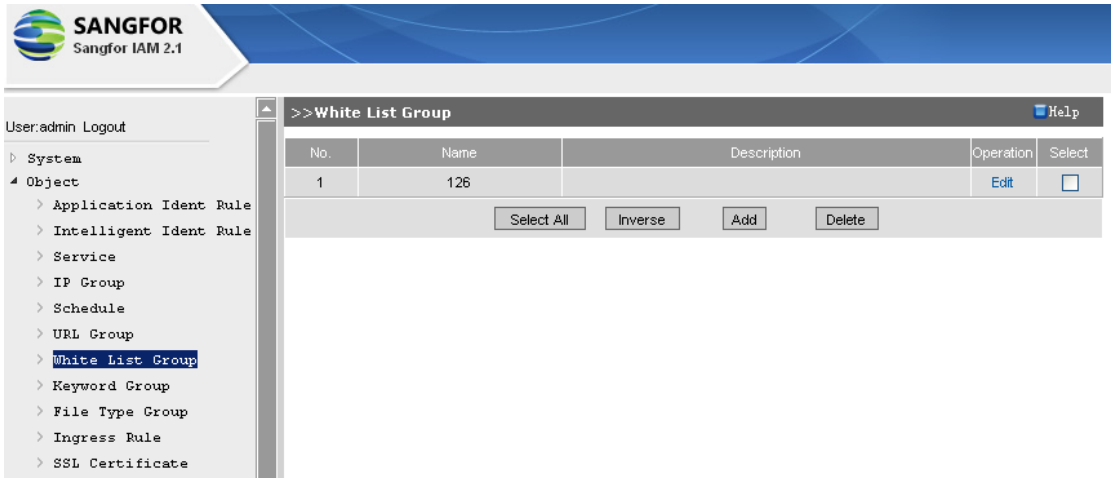
[Add URL]: Type in a domain name (URL) into the [Add URL] text box and click the <Add> button followed to add this domain name into the list, one entry (URL) per row.

[Domain Name Keyword]: URL group is automatically matched if the URL contains the configured domain name keyword.

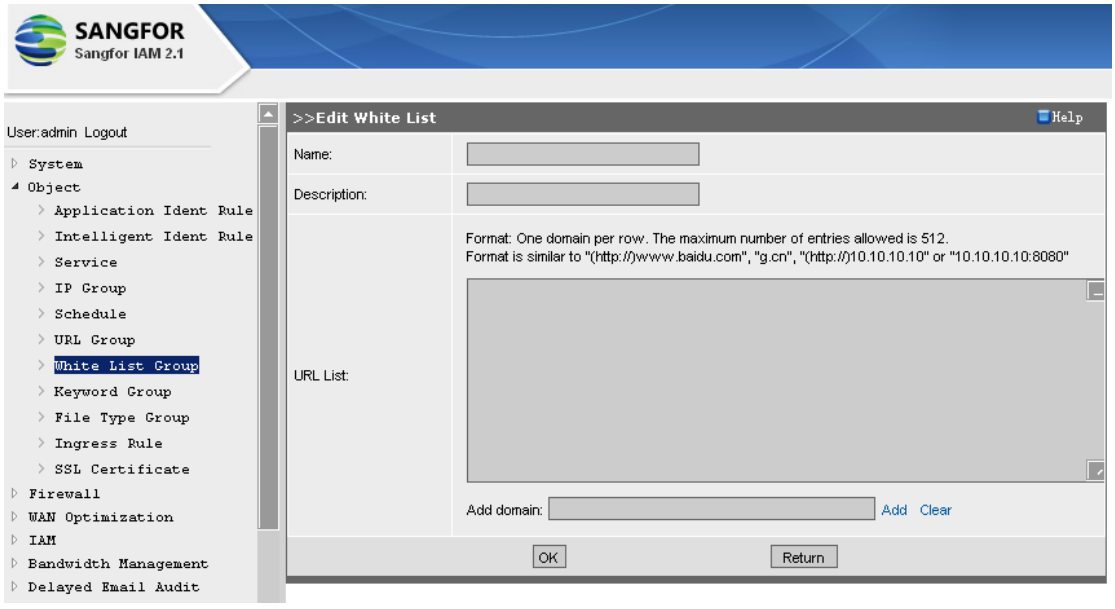
Having completed configuring this page, you have to click the <OK> button to save the settings.

4.7. White List Group

[White List Group] defines the domain name white list, which can be referenced by [Access Control Policy] > [Edit Access Control Policy] > [Web Filter] > [File Type Filter], [ActiveX Filter] and [Scrip Filter].



Under the default configuration page (above), click the <Add> button to enter the [Edit White List] page, as shown below:



[Name]: Names the new white list group.

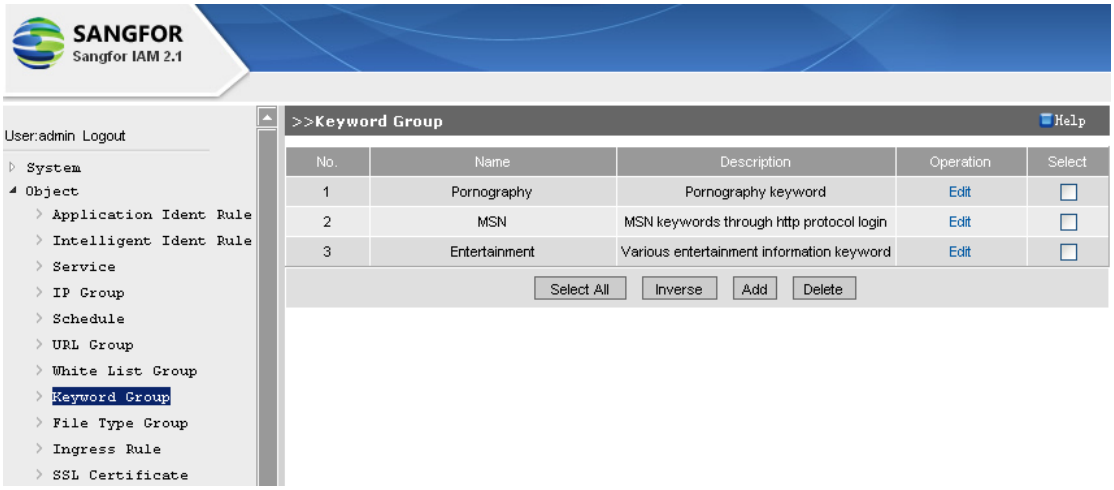
[Description]: Type in a brief description for this white list group.

[URL List]: Configures the composition of the white list group, one domain name (IP address) per row.

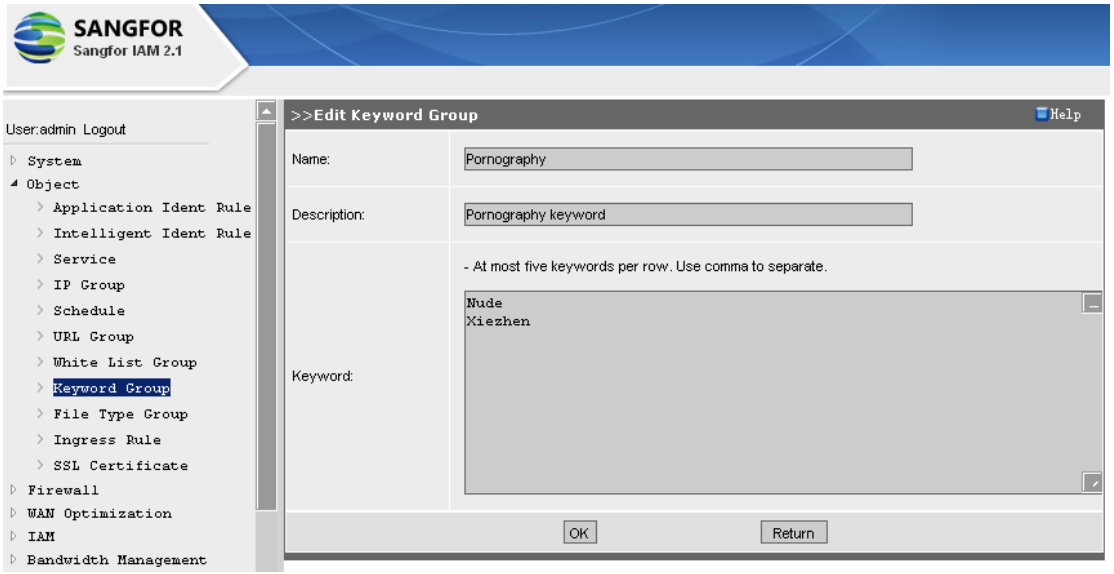
Having completed configuring, you have to click the <OK> button to save the settings.

4.8. Keyword Group

[Keyword Group] is used for configuring and classifying the keywords. The [Keyword Groups] can be referenced by [IAM] > [Access Control Policy] > [Edit Access Control Policy] page > [Web Filter] > [Keyword Filter] to control searching and uploading information that contains the keywords in the keyword group.



Under the [Keyword Group] default configuration page, click the <Add> button to enter the [Edit Keyword Group] page, as shown below:



[Name]: Names the new keyword group.

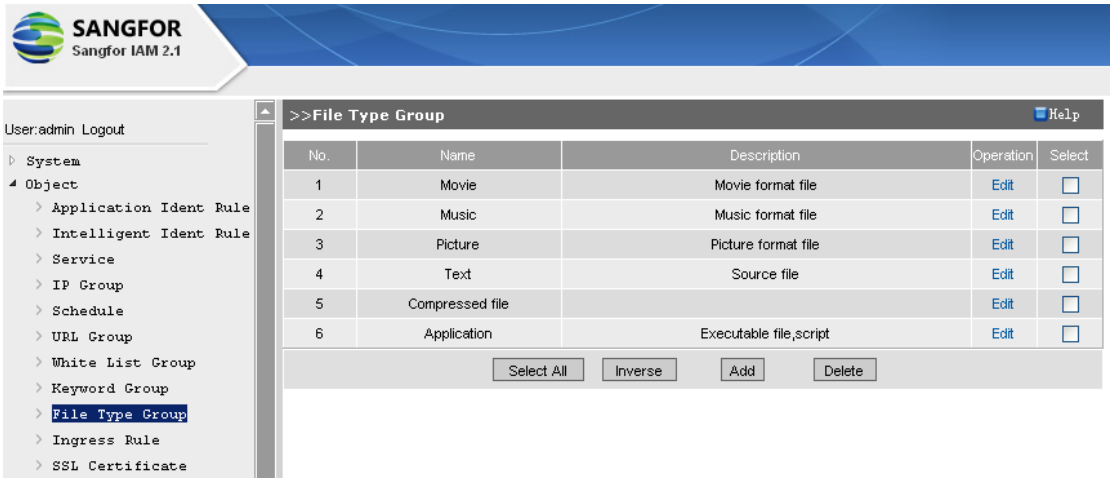
[Description]: Type in a brief description for this keyword group.

[Keyword]: Configures the keywords, one entry (keyword) per row.

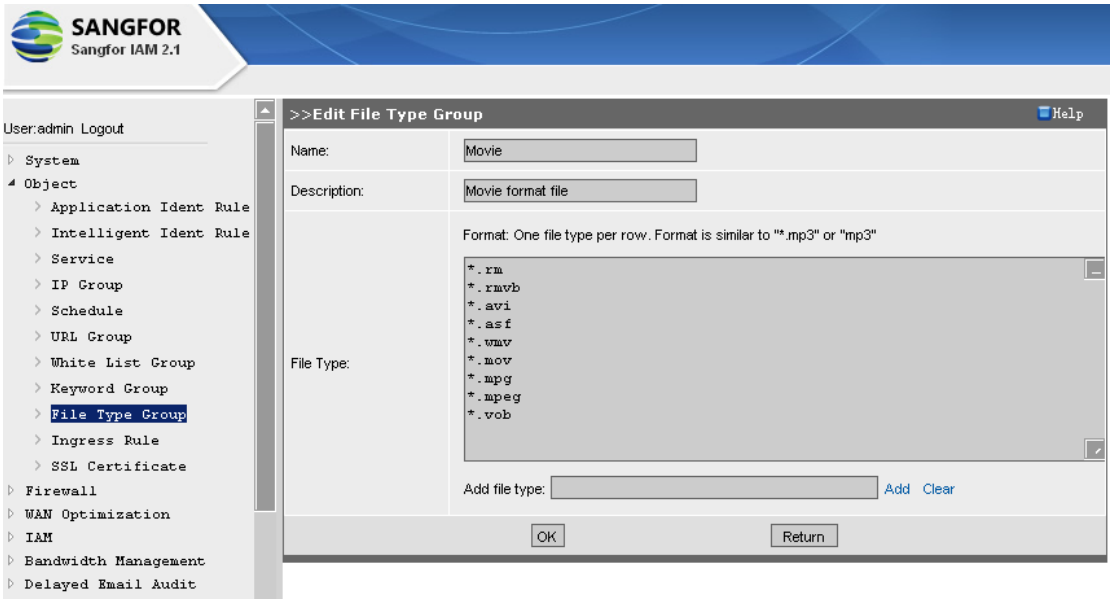
Having completed configuring, you have to click the <OK> button to save the settings.

4.9. File Type Group

[File Type Group] defines the needed file types. [File Type Group] can be referenced by [IAM] > [Access Control Policy] > [Edit Access Control Policy] page > [Web Filter] > [File Type Filter] to control HTTP and FTP upload and download, and can be referenced by [Bandwidth Management] > [Bandwidth Settings] page > [Bandwidth Channel] to control the upload and download bandwidth of the configured file types (in the file type group).



Under the default configuration page, click the <Add> button to enter the [Edit File Type Group] default configuration page, as shown below:



[Name]: Names the new file type group.

[Description]: Type in a brief description for this file type group.

[File Type]: Configures the extension of file type, one entry per row.

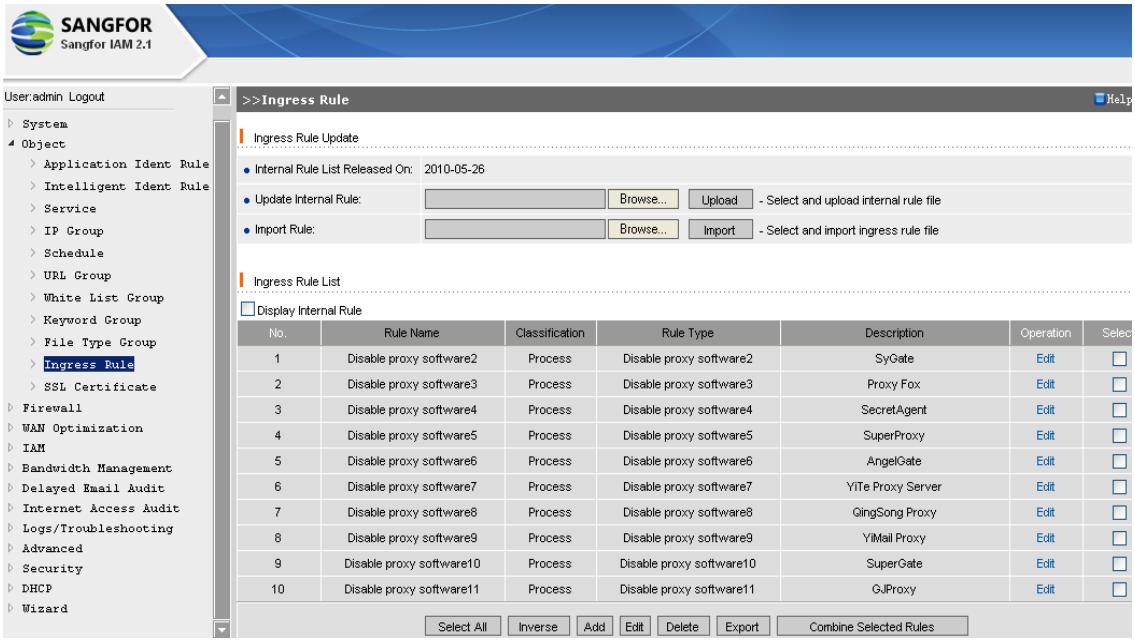
Having completed configuring, you have to click the <OK> button to save the settings.

Extension name of a file type cannot be entered twice or more.

4.10. Ingress Rule

[Ingress Rule] configures the rules to be applied when users get access to the Internet. The ingress rules are to ban the use of proxy software, bind IP/MAC address of three layers and monitor encrypted IM message, and can be referenced by [IAM] > [Access Control Policy] > [Edit Access Control Policy] page > [Ingress Rule]. If the access control policy has referenced ingress rule(s), users have to satisfy the corresponding rules to access the Internet, and install the ActiveX control when getting access to the Internet for the first time.

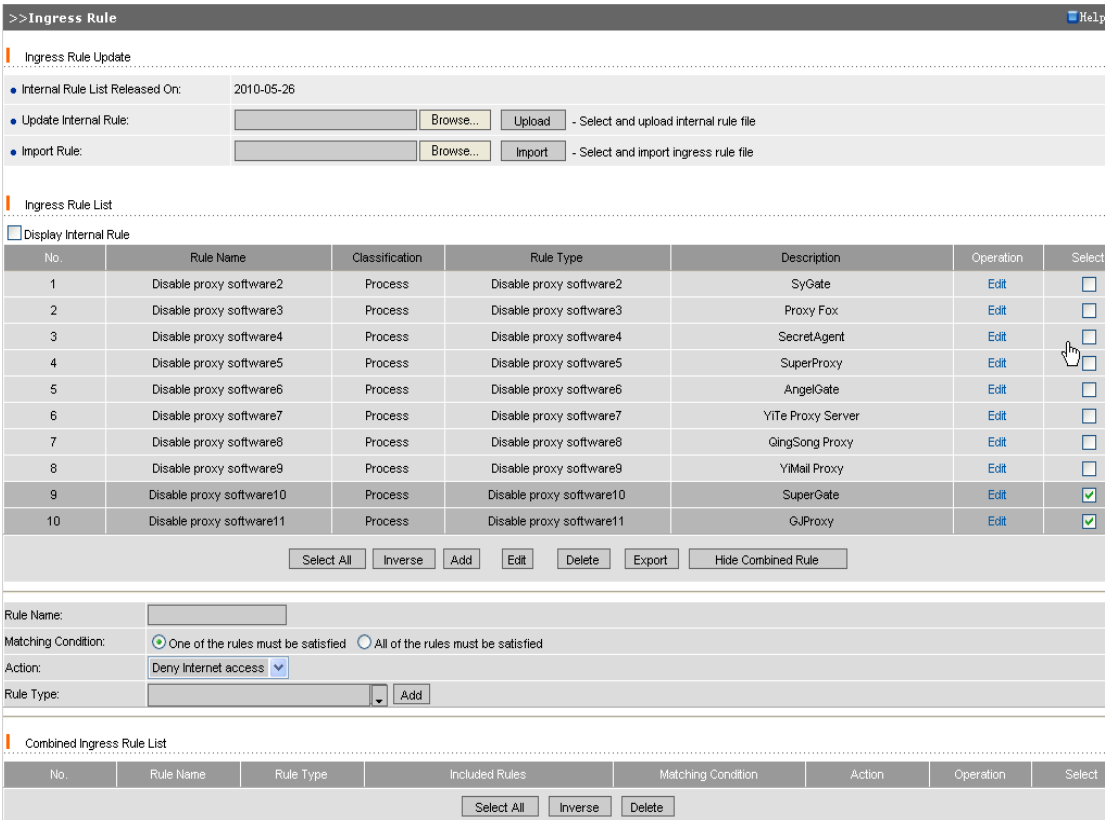
IAM gateway device is built in with some ingress rules; you can define ingress rule(s) by yourself.


SANGFOR
Sangfor IAM 2.1
User:admin Logout
System
Object
Application Ident Rule
Intelligent Ident Rule
Service
IP Group
Schedule
URL Group
White List Group
Keyword Group
File Type Group
Ingress Rule
SSL Certificate
Firewall
WAN Optimization
IAM
Bandwidth Management
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Security
DHCP
Wizard
>>Ingress Rule
Help
Ingress Rule Update
Internal Rule List Released On: 2010-05-26
Update Internal Rule: Browse... Upload - Select and upload internal rule file
Import Rule: Browse... Import - Select and import ingress rule file
Ingress Rule List
Display Internal Rule
No. Rule Name Classification Rule Type Description Operation Selec
1 Disable proxy software2 Process Disable proxy software2 SyGate Edit
2 Disable proxy software3 Process Disable proxy software3 Proxy Fox Edit
3 Disable proxy software4 Process Disable proxy software4 SecretAgent Edit
4 Disable proxy software5 Process Disable proxy software5 SuperProxy Edit
5 Disable proxy software6 Process Disable proxy software6 AngelGate Edit
6 Disable proxy software7 Process Disable proxy software7 YiTe Proxy Server Edit
7 Disable proxy software8 Process Disable proxy software8 QingSong Proxy Edit
8 Disable proxy software9 Process Disable proxy software9 YiMail Proxy Edit
9 Disable proxy software10 Process Disable proxy software10 SuperGate Edit
10 Disable proxy software11 Process Disable proxy software11 GJProxy Edit
Select All Inverse Add Edit Delete Export Combine Selected Rules

[Update Internal Rule]: Click the <Browse> button to upload the internal ingress rule file and update the current internal rules. You can obtain this file from SANGFOR Customer Service.

[Import Rule] is corresponding to the <Export> button below the [Ingress Rule List] which can export the selected ingress rule file(s) of .conf format; while the <Import> button is used for importing the uploaded .conf format rule file into the system.

<Combine Selected Rules>: Select two or more ingress rules and click this button to combine the selected rules, as shown below:


>>Ingress Rule
Help
Ingress Rule Update
Internal Rule List Released On: 2010-05-26
Update Internal Rule: Browse... Upload - Select and upload internal rule file
Import Rule: Browse... Import - Select and import ingress rule file
Ingress Rule List
Display Internal Rule
No. Rule Name Classification Rule Type Description Operation Select
1 Disable proxy software2 Process Disable proxy software2 SyGate Edit
2 Disable proxy software3 Process Disable proxy software3 Proxy Fox Edit
3 Disable proxy software4 Process Disable proxy software4 SecretAgent Edit
4 Disable proxy software5 Process Disable proxy software5 SuperProxy Edit
5 Disable proxy software6 Process Disable proxy software6 AngelGate Edit
6 Disable proxy software7 Process Disable proxy software7 YiTe Proxy Server Edit
7 Disable proxy software8 Process Disable proxy software8 QingSong Proxy Edit
8 Disable proxy software9 Process Disable proxy software9 YiMail Proxy Edit
9 Disable proxy software10 Process Disable proxy software10 SuperGate Edit
10 Disable proxy software11 Process Disable proxy software11 GJProxy Edit
Select All Inverse Add Edit Delete Export Hide Combined Rule
Rule Name:
Matching Condition: One of the rules must be satisfied All of the rules must be satisfied
Action: Deny Internet access
Rule Type: Add
Combined Ingress Rule List
No. Rule Name Rule Type Included Rules Matching Condition Action Operation Select
Select All Inverse Delete

[Rule Name]: Names the combined ingress rule.

[Matching Condition]: Select the matching condition to the combined rule, [One of the rules must be satisfied] or [All of the rules must be satisfied].

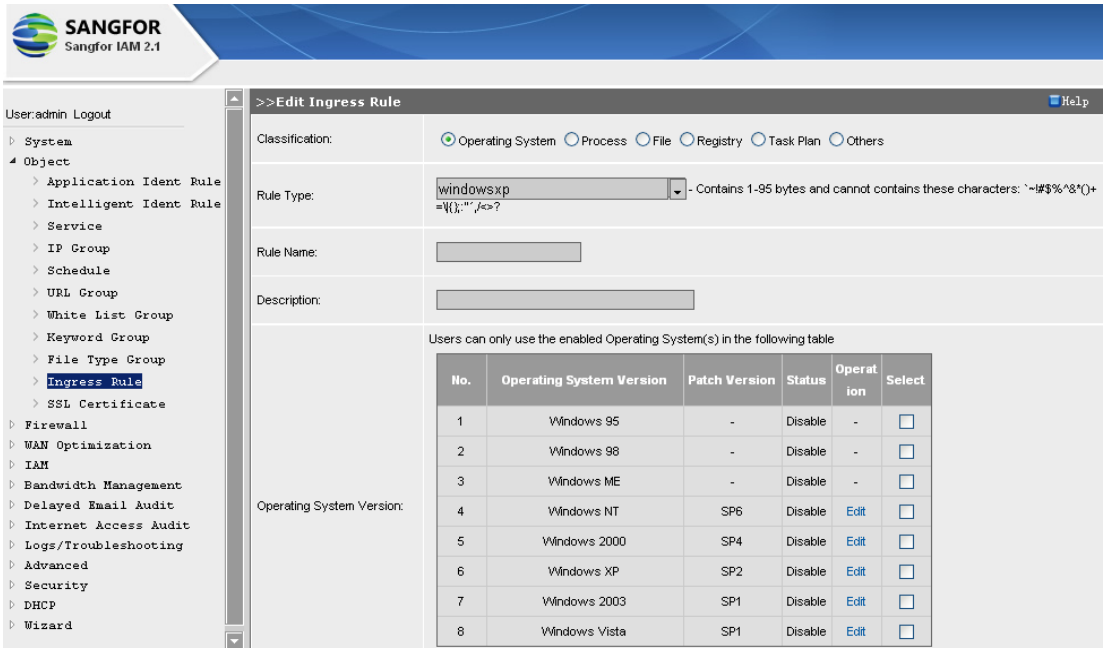
[Matching Condition]: Defined the relations between the combined rules. Options are [One of the rules must be satisfied] and [All of the rules must be satisfied].

[Action]: Select the action if the [Matching Condition] is satisfied. Options are [Deny Internet access] and [Submit report only].

[Rule Type]: Defines the type of this combined rule.

Having completed configuring the above, you have to click the <Add> button to add this combined rule to the [Combined Ingress Rule List].

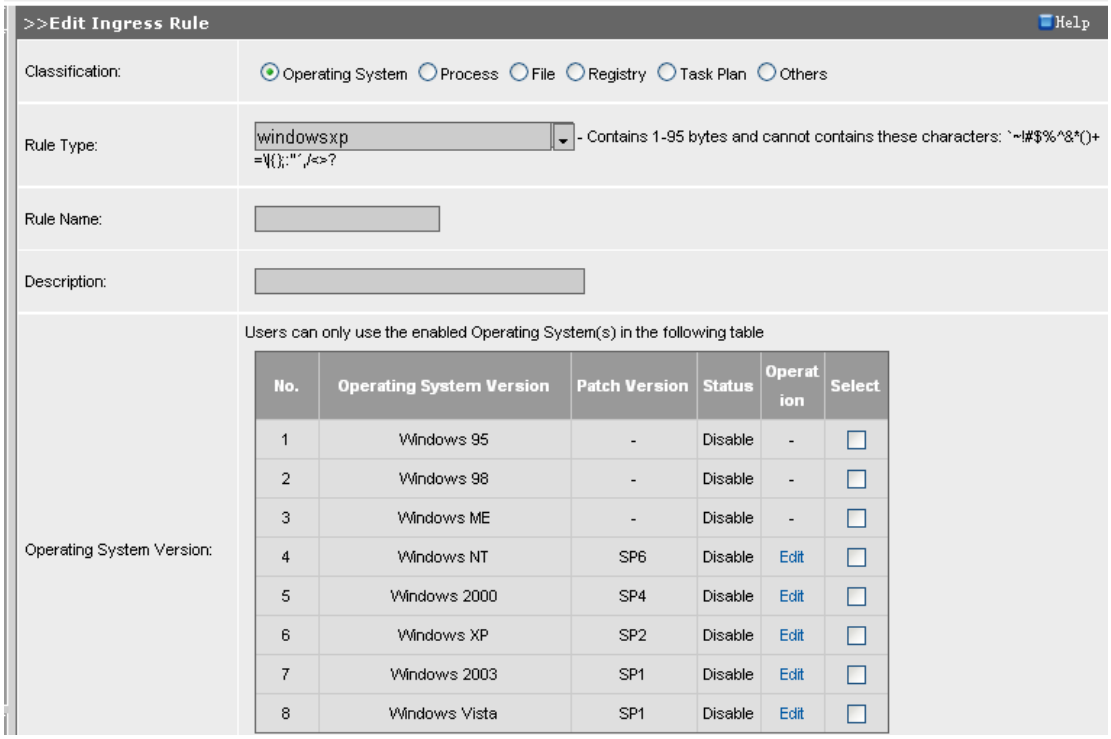
To create a new ingress rule, click the <Add> button (below the [Ingress Rule List]) to enter the [Edit Ingress Rule] configuration page, as shown below:



[Classification]: Defines the classification of this ingress rule; options are [Operation System], [Process], [File], [Registry], [Task Plan] and [Others].

[Rule Type]: Select the type for this ingress rule (or enter directly a new user-defined rule type name into the text box followed).

[Operating System] ingress rule specifies the operating system of the LAN computer which is going to get access to the Internet through the IAM gateway device. For instance, if the LAN computers of an enterprise use the Microsoft Windows XP, in order to prevent the LAN users from infecting virus who do not download the SP2 patch, we take the following measures: IAM gateway device monitors all the Internet access data packets from the LAN PCs, the PCs that have downloaded the SP2 patch can get access, while the PCs that have not downloaded the SP2 patch cannot access the Internet. Detailed configuring procedures are as shown below:



Step 1: <Add> a new ingress rule. Select [Classification] (or any other existing rule type).

Step 2: Enter [Rule type]. Click the pull-down menu and select a rule type, or enter a new one. Length of rule type must be within 95 bytes.

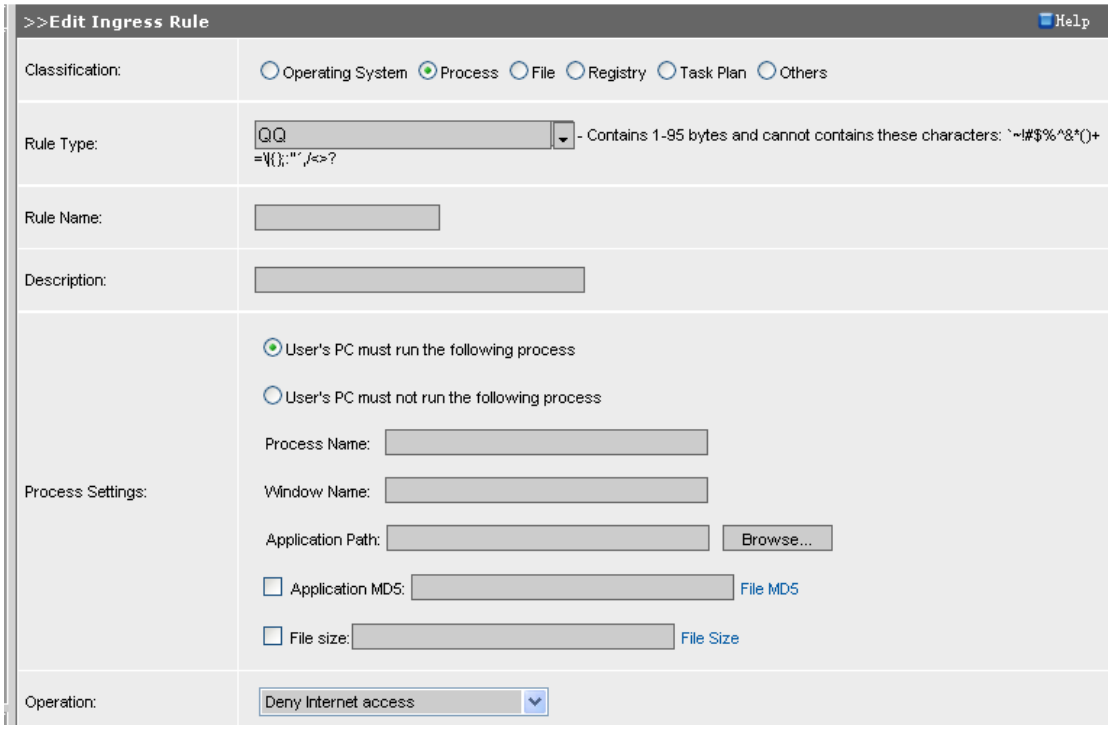
Step 3: Enter [Rule Name]. Length of a rule name must be within 95 bytes.

Step 4: Select [Operating System Version]. If no operating system version is selected, this ingress rule will ban the user from accessing Internet. First, select operation version(s) and then click <Enable> to enable this OS version.

Step 5: Select [Action], to [Deny Internet access] or [Submit report only].

Step 6: Click the <OK> button to enable this ingress rule.

[Process] ingress rule controls the process on the LAN computers that are getting access to the Internet. Click the <Add> button and create a new ingress rule of [Process], the page is as shown below:

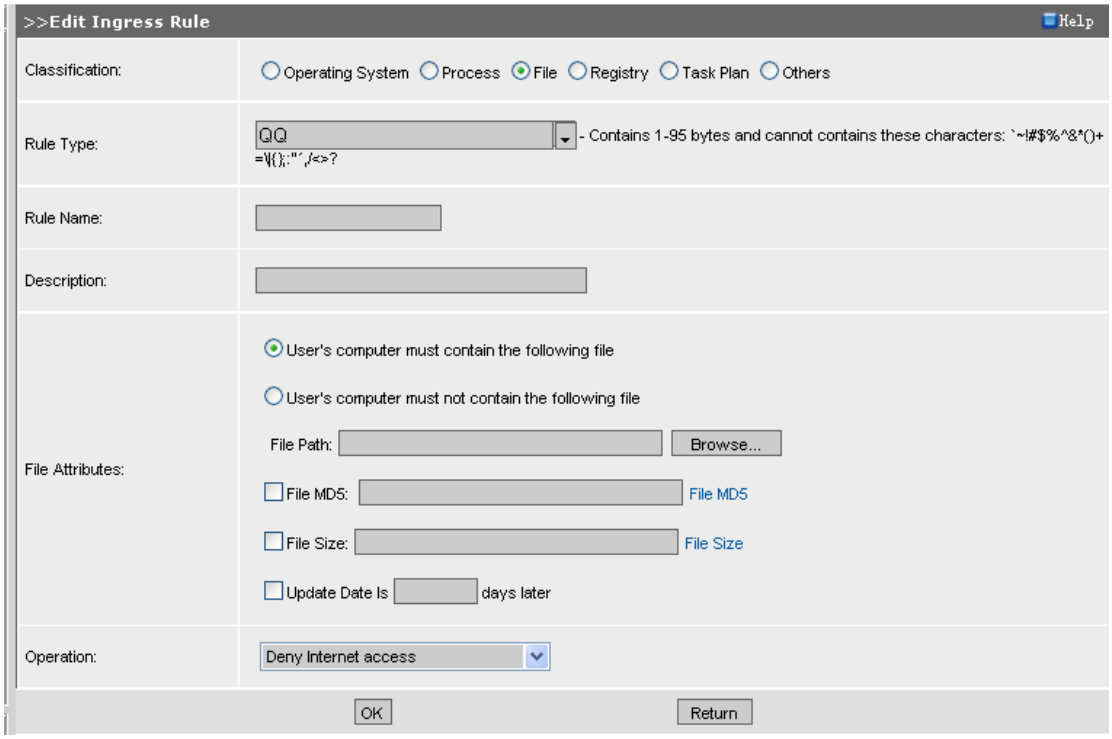


Configure [Rule Type], [Rule Name], [Description], [Process Settings] (including [Process Name], [Window Name], [Application Path], [Application MD5], [File Size], etc.), and [Operation] as [Deny Internet access], [Stop Process] or [Submit report only]

Having completed configuring this page, click the <OK> button to save the settings and add this ingress rule to the [Ingress Rule List].

[File] ingress rule controls the files of the LAN computers who get access to the Internet through the IAM gateway device. If you enabled this type of ingress rule, the IAM gateway will detect whether there is certain file (for instance .dll file) and therefore check whether the LAN computer has installed the specific software.

Configuration page of [File] ingress rule is as shown below:



Configure [Rule Type], [Rule Name], [Description]

[File Attributes]: Options are [User's computer must contain the following file] and [User's computer must not contain the following file]; enter the file path or click <Browse> to upload the file; check and calculate the [File MD5], [File Size] and [Update Date is _ days later]. Select an [Operation].

[Update Date is _ days later]: Indicates whether the antivirus software of the LAN computer is updated or not, and for how many days the antivirus software on the LAN computer has lagged behind to be updated. If the time is longer than the days configured here, the IAM gateway device will take the corresponding operation.

Having completed configuring this page, click the <OK> button to save the settings and add this rule to the [Ingress Rule List]

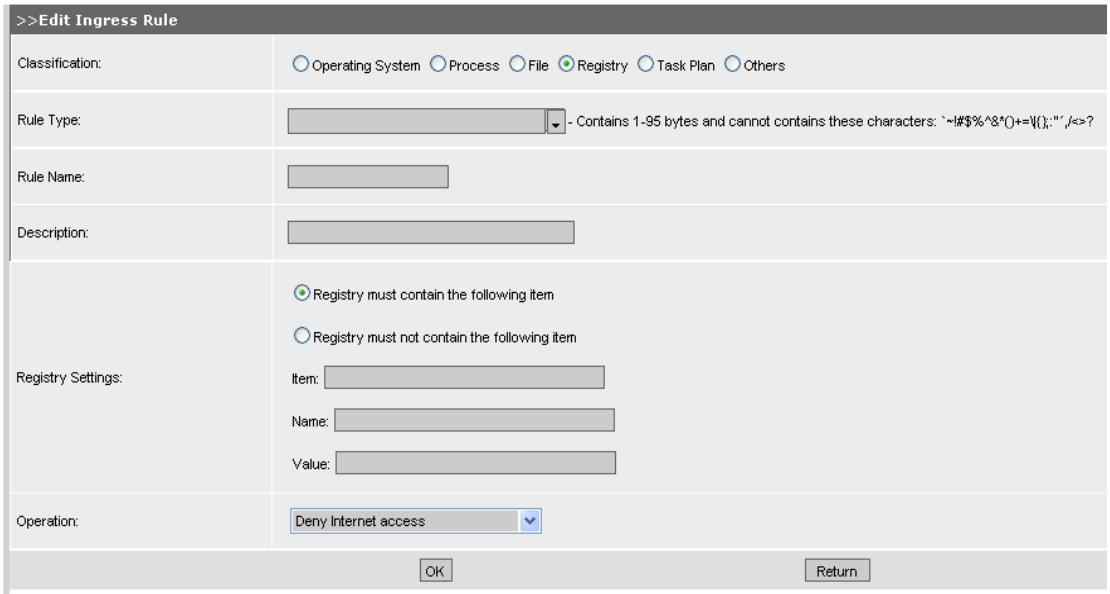
- [File Path] can be translated, for instance, %SystemRoot% indicates where the Windows system directory is (provided the C disk is the system disk), generally C:\WINDOWS or C:\WINNT. Since the software files are installed in different subdirectories, macro directory translation makes sense.
- If you are adding a [File] ingress rule, yon can use the macro directory translation function to

type the [File Path] that is provided by IAM gateway device. Definitions of some the macro directories are as shown in the following table (case insensitive):

Format	Definition (provided the C disk is the system disk)
%SystemDrive%	C:
%SystemRoot%	C:\WINNT
%System%	C:\WINNT\system32
%Windir%	C:\WINNT
%UserProfile%	C:\Documents and Settings\SINFOR
%Temp%	C:\Documents and Settings\SINFOR\Local Settings\Temp
%Program%	C:\Program Files

[Registry] ingress rule checks the Registry of the operating system of the LAN computer that gets access to the Internet through the IAM gateway device. In this way, it can find the software and security problems of the software of the operating system.

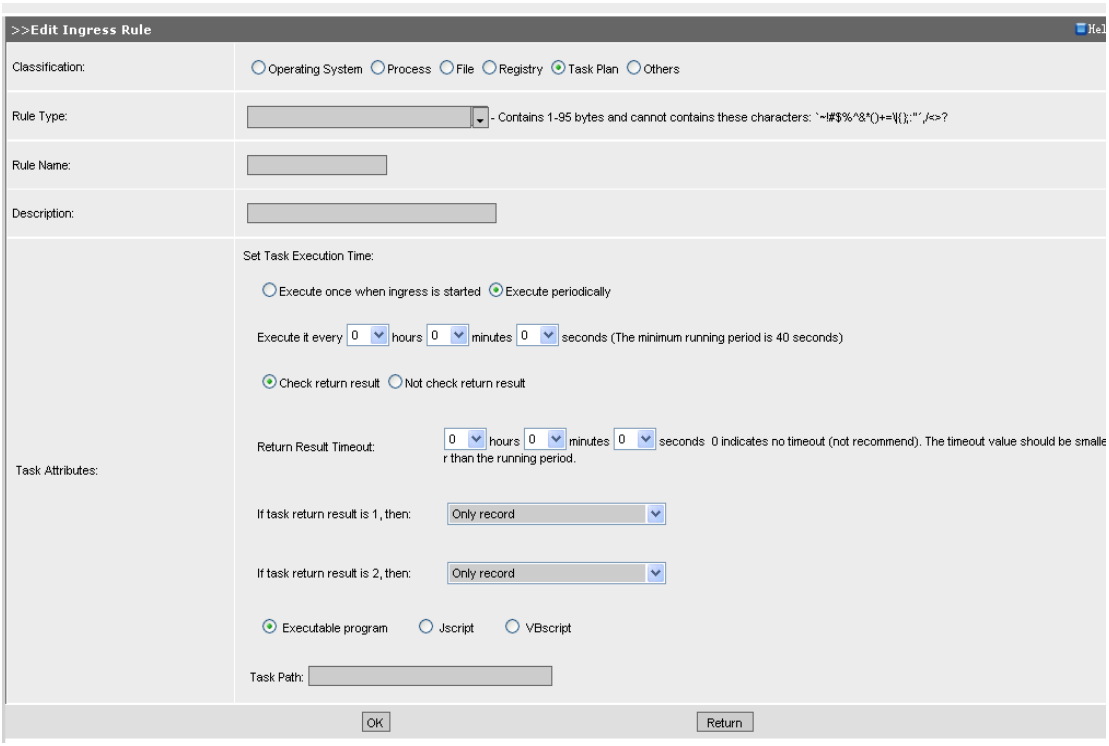
The configuration page of the [Registry] ingress rule is as shown below:



[Task Plan] ingress rule configures the script and program that the client terminal may run (the script and program is user-defined); the IAM gateway device then can control the Internet access

with the return value.

The [Task Plan] ingress rule configuration page is as shown below:



[Rule Type]: Configures the type of the ingress rule.

[Rule Name], [Description]: Configures the name and brief description for the ingress rule.

[Task Attributes]: Configures the task execution time, [Execute once when ingress is started] or [Execute periodically].

If the [Execute periodically] is selected, you can configure the interval for periodic execution, as shown in the figure above.

[Check return result], [Not check return result]: Configures whether to check the execution results of the task script.

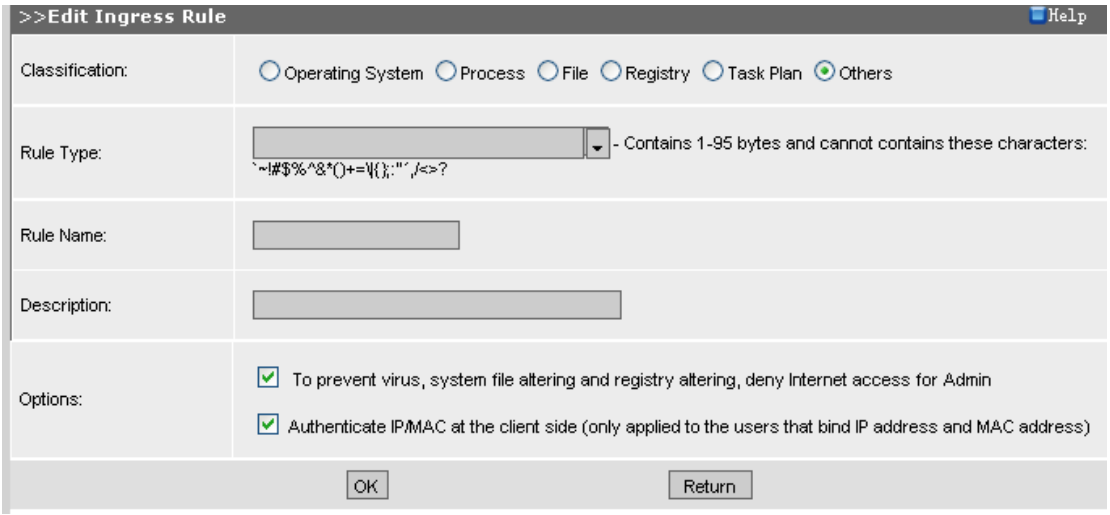
[Return Result Timeout]: Configures the timeout for obtaining the return results.

[If task return result is 1, then], [If task return result is 2, then]: Configures the operation taken if the obtained task script is incoherent to the return results. It may [Only record], or [Prompt user], or [Deny Internet Access], or [Deny Internet access/prompt user]. Presently, only some of the scripts are supported, namely, [Executable program], [Jscript] and [VBscript].

[Task Path]: Type in the detailed path where the task script is saved in the local client-end PC.

[Others] ingress rule can fulfill IP/MAC binding over the layer 3 switch, and ban the client end from logging into a LAN PC as administrator to access the Internet, which can avoid virus infection.

The [Others] ingress rule configuration page is as shown below:



Configure [Rule Type], [Rule Name], [Description], etc.

[Options]: Check [Authenticate IP/MAC at the client side] to realize IP/MAC binding over the layer 3 switch; check [To prevent virus, system file altering and registry altering, deny Internet access for Admin] to ban the client end from logging in to a LAN PC as administrator to get access to the Internet.

Having completed configuring this page, you have to click the <OK> button to save the settings and add the ingress rule to the [Ingress Rule List].

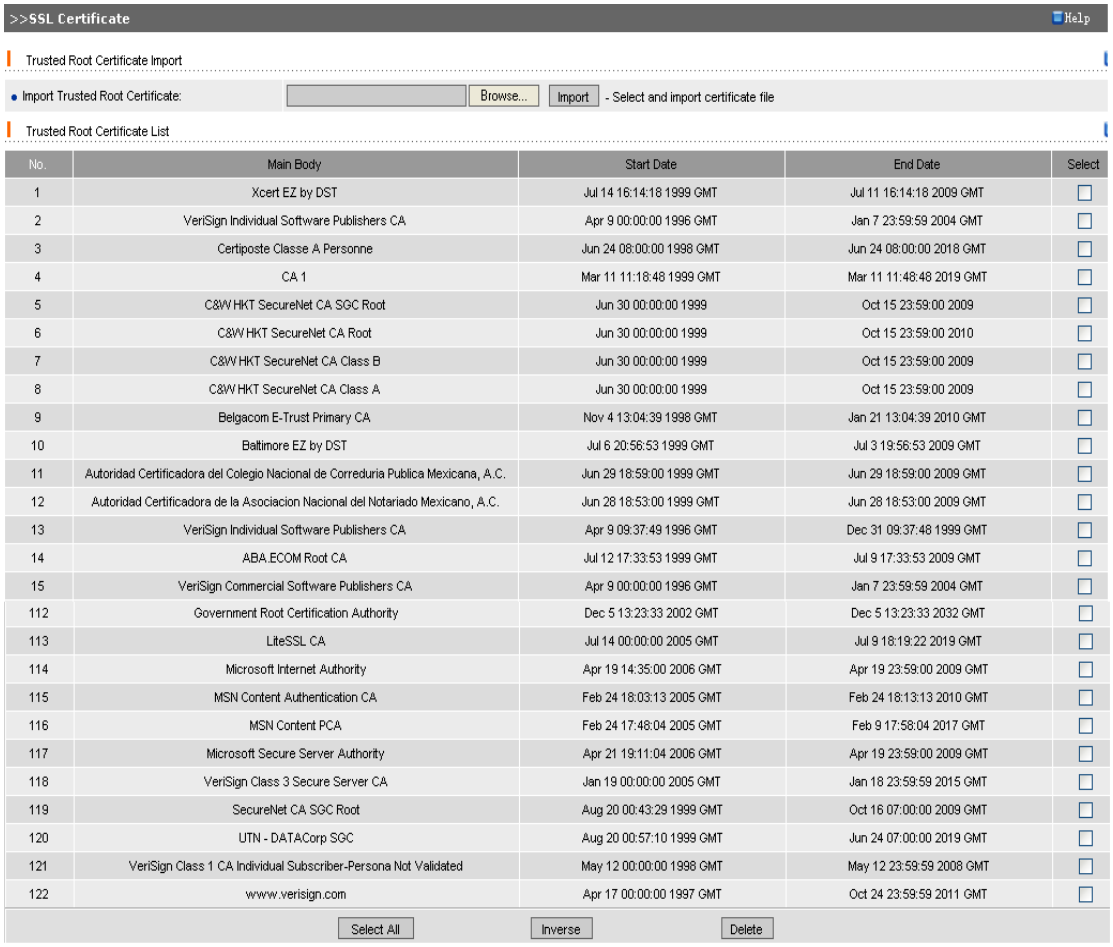
The condition for applying ingress rule to bind IP/MAC is that, the PC and the IAM gateway device must be at different subnet segments (crossing a layer 3 switch and the MAC address changed). In addition to the settings configured here, IP/MAC binding must be configured in [IAM] > [Organization Structure] > [Edit User] page > [Advanced Settings] > [User Attribute]. For details, please refer to Section 7.4.5.1 Edit User.

4.11. SSL Certificate

[Trusted Root Certificate List] is coherent to [IAM] > [Access Control Policy] > [Edit Access Control Policy] > [SSL Management] > [SSL Control]. If the [SSL Control] is enabled, then the

root certificates in the library are trusted. You can import trusted root certificate to the [Trusted Root Certificate List] or delete a trusted root certificate.

The related page is as shown below:


>>SSL Certificate
Help
Trusted Root Certificate Import
Import Trusted Root Certificate:
Browse...
Import
- Select and import certificate file
Trusted Root Certificate List
No.
Main Body
Start Date
End Date
Select
1 Xcert EZ by DST Jul 14 16:14:18 1999 GMT Jul 11 16:14:18 2009 GMT
2 VeriSign Individual Software Publishers CA Apr 9 00:00:00 1996 GMT Jan 7 23:59:59 2004 GMT
3 Certiposte Classe A Personne Jun 24 08:00:00 1998 GMT Jun 24 08:00:00 2018 GMT
4 CA 1 Mar 11 11:18:48 1999 GMT Mar 11 11:48:48 2019 GMT
5 C&W HKT SecureNet CA SGC Root Jun 30 00:00:00 1999 Oct 15 23:59:00 2009
6 C&W HKT SecureNet CA Root Jun 30 00:00:00 1999 Oct 15 23:59:00 2010
7 C&W HKT SecureNet CA Class B Jun 30 00:00:00 1999 Oct 15 23:59:00 2009
8 C&W HKT SecureNet CA Class A Jun 30 00:00:00 1999 Oct 15 23:59:00 2009
9 Belgacom E-Trust Primary CA Nov 4 13:04:39 1998 GMT Jan 21 13:04:39 2010 GMT
10 Baltimore EZ by DST Jul 6 20:56:53 1999 GMT Jul 3 19:56:53 2009 GMT
11 Autoridad Certificadora del Colegio Nacional de Correduria Publica Mexicana, A.C. Jun 29 18:59:00 1999 GMT Jun 29 18:59:00 2009 GMT
12 Autoridad Certificadora de la Asociacion Nacional del Notariado Mexicano, A.C. Jun 28 18:53:00 1999 GMT Jun 28 18:53:00 2009 GMT
13 VeriSign Individual Software Publishers CA Apr 9 09:37:49 1996 GMT Dec 31 09:37:48 1999 GMT
14 ABA.ECOM Root CA Jul 12 17:33:53 1999 GMT Jul 9 17:33:53 2009 GMT
15 VeriSign Commercial Software Publishers CA Apr 9 00:00:00 1996 GMT Jan 7 23:59:59 2004 GMT
112 Government Root Certification Authority Dec 5 13:23:33 2002 GMT Dec 5 13:23:33 2032 GMT
113 LiteSSL CA Jul 14 00:00:00 2005 GMT Jul 9 18:19:22 2019 GMT
114 Microsoft Internet Authority Apr 19 14:35:00 2006 GMT Apr 19 23:59:00 2009 GMT
115 MSN Content Authentication CA Feb 24 18:03:13 2005 GMT Feb 24 18:13:13 2010 GMT
116 MSN Content PCA Feb 24 17:48:04 2005 GMT Feb 9 17:58:04 2017 GMT
117 Microsoft Secure Server Authority Apr 21 19:11:04 2006 GMT Apr 19 23:59:00 2009 GMT
118 VeriSign Class 3 Secure Server CA Jan 19 00:00:00 2005 GMT Jan 18 23:59:59 2015 GMT
119 SecureNet CA SGC Root Aug 20 00:43:29 1999 GMT Oct 16 07:00:00 2009 GMT
120 UTN - DATACorp SGC Aug 20 00:57:10 1999 GMT Jun 24 07:00:00 2019 GMT
121 VeriSign Class 1 CA Individual Subscriber-Persona Not Validated May 12 00:00:00 1998 GMT May 12 23:59:59 2008 GMT
122 www.verisign.com Apr 17 00:00:00 1997 GMT Oct 24 23:59:59 2011 GMT
Select All
Inverse
Delete

[Import Trusted Root Certificate]: Import certificate from the local PC, only support crt or cer format certificate.

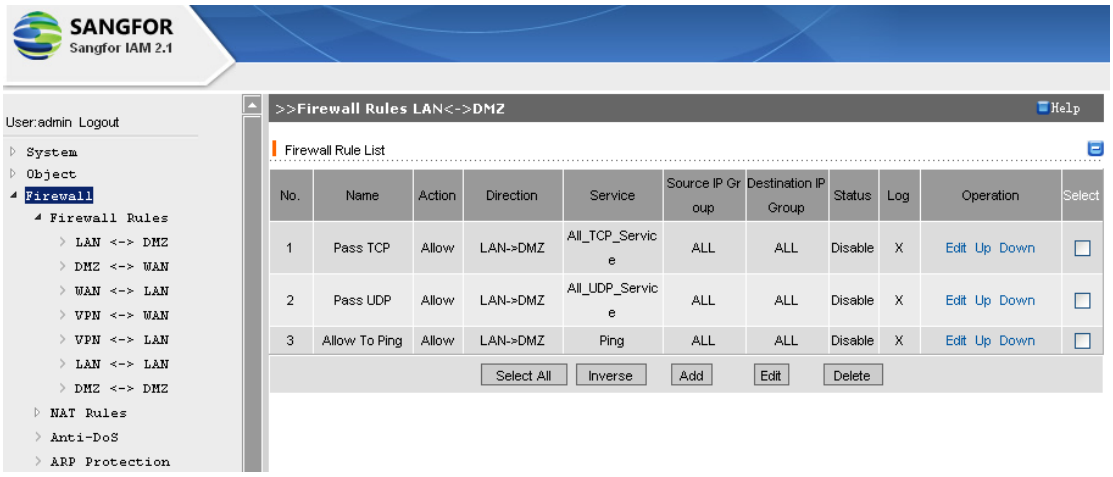
Differentiation of different certificates is inspected by MD5 value of the certificate. If the MD5 value of a certification is different from others, then it is regarded as another certificate.

A certificate cannot be imported twice or more.

Generally, name of the certificate main body is the corresponding CN name of the certificate subject in IE. If the certificate subject contains no CN name, it will take the last field of the subject as the main body of the certificate (the field order may be different from that of IE).

Chapter 5 Firewall

[Firewall] covers configurations of [Firewall Rules], [NAT Rules], [Anti-DoS] and [ARP Protection], as shown below:



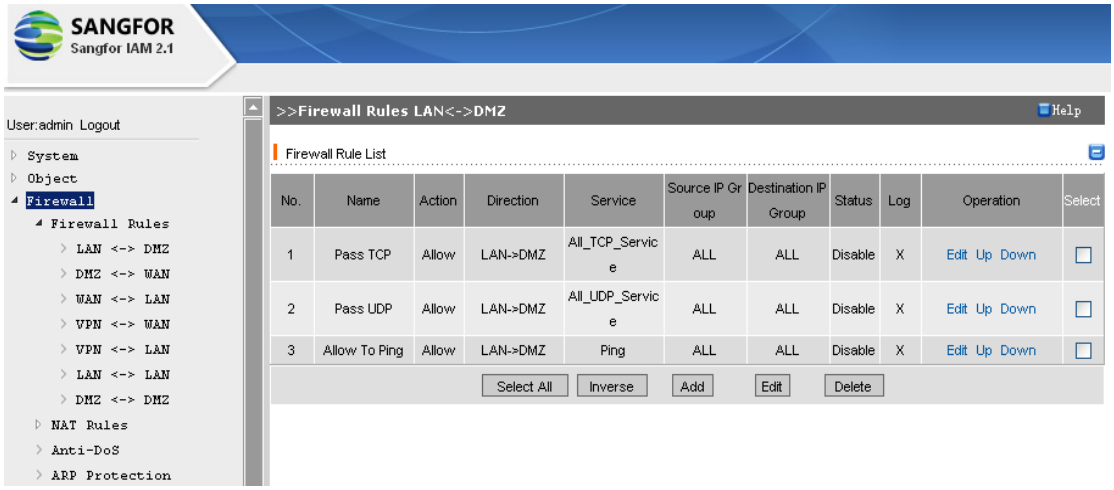
5.1. Firewall Rule

[Firewall Rule] configures the specific settings of data packet access. IAM gateway device allows you to configure the filtering rules for data transmission between [LAN<->DMZ], [DMZ<->WAN], [WAN<->LAN], [LAN<->LAN], [DMZ<->DMZ], [VPN<->WAN] and [VPN<->LAN].

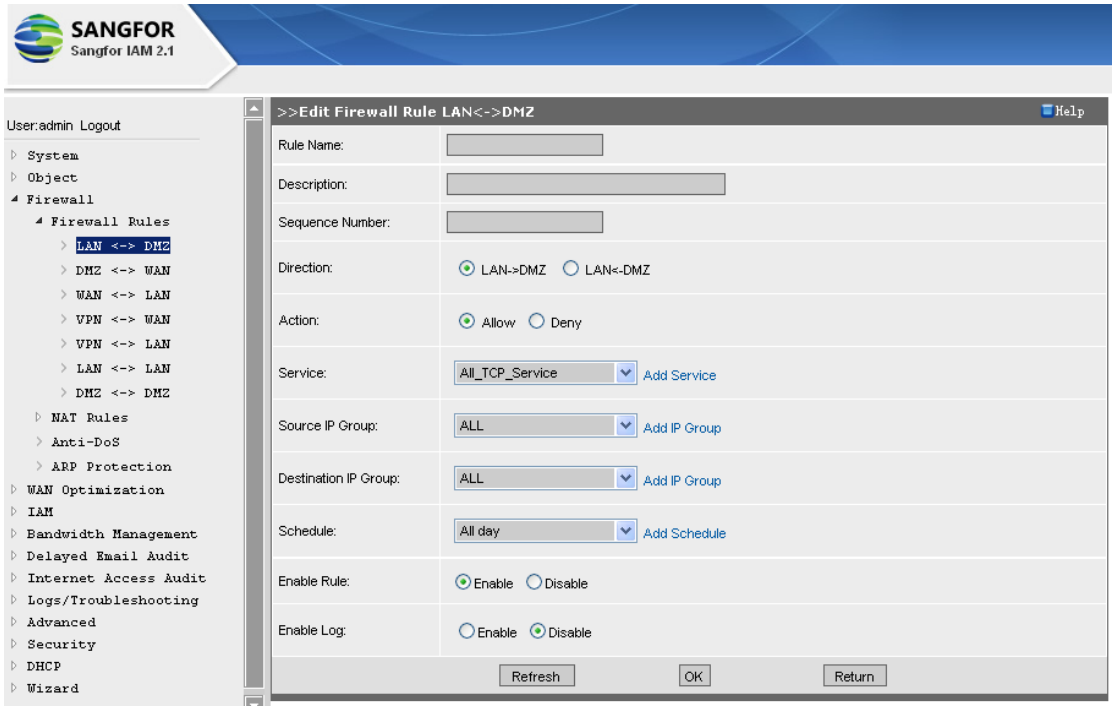
5.1.1. LAN <-> DMZ

[LAN <-> DMZ] configures the rule for data transmission fulfilled between LAN interface and DMZ interface. The service can be all the services of certain protocol or a user-defined service.

For example, to have the communication between the LAN interface and DMZ interface available, you have to enable all the TCP, UDP and ICMP services and have them available for both directions, LAN > DMZ and DMZ > LAN. By default, all the TCP, UDP, ICMP services are accessible for [LAN->DMZ]; however, if the rule is not enabled, the [Status] displayed in the [Firewall Rule List] is [Disable], as shown below:



Under the above configuration page, click the <Edit> button and the [Edit Firewall Rule LAN<->DMZ] configuration page. Click the <Enable> button to enable this rule; or click the <Add> button and the [Edit Firewall Rule LAN<->DMZ] configuration page pops up, as shown in the following figure:



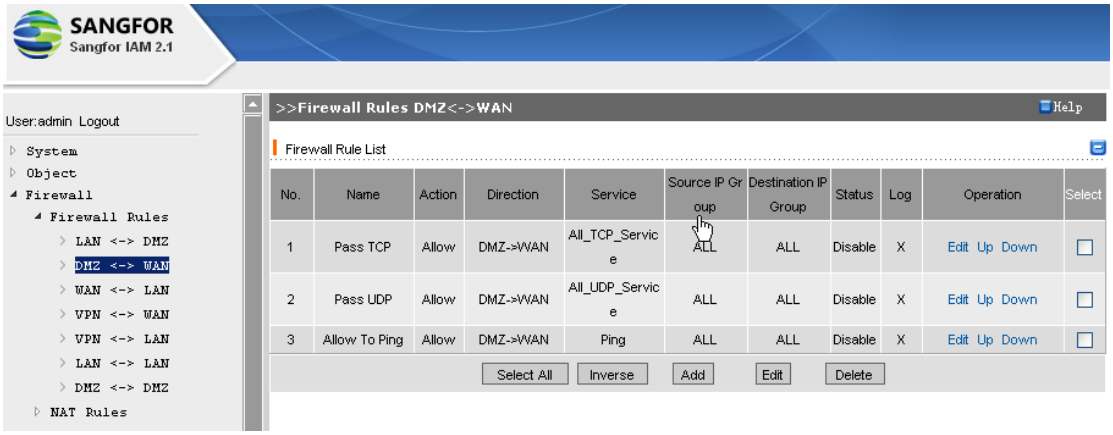
- Firewall rules are to be matched from top to bottom. If a rule is matched, the rules below it will not to be matched, therefore, please arrange the rules in needed order. Order arrangement of the firewall rules cannot only be fulfilled through the [Firewall Rule List], but be numbered by [Sequence Number] (in the above figure).
- The Firewall defaults to deny the data packets if none of the firewall rules is matching, that is

to say, the data packets will be dropped.

5.1.2. DMZ <-> WAN

[DMZ <-> WAN] configures the rule for access fulfilled between WAN interface and DMZ interface. The service can be all the services of certain protocol or a user-defined service(s). For detailed configuration, please refer to Section 5.1.1 LAN <-> DMZ.

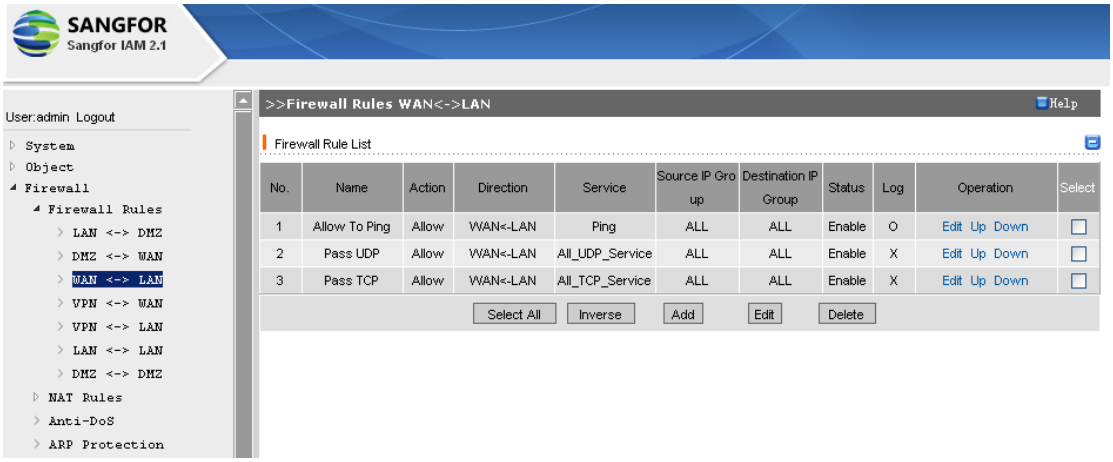
The default configuration page is as shown below:



5.1.3. WAN<->LAN

[WAN <-> LAN] page configures the rule communication between the LAN interface and the WAN interface. By default, Internet access through the LAN interface has no limitation, while LAN access through the WAN interface is not allowed. To enable the external network to access a local area network, you have to configure a filtering rule which allows the Internet IP to access the LAN IP address.

As shown in the figure below, the port configured for Internet IP to access the local area network is 80, which indicates the port for communication from [WAN->LAN] is 80.



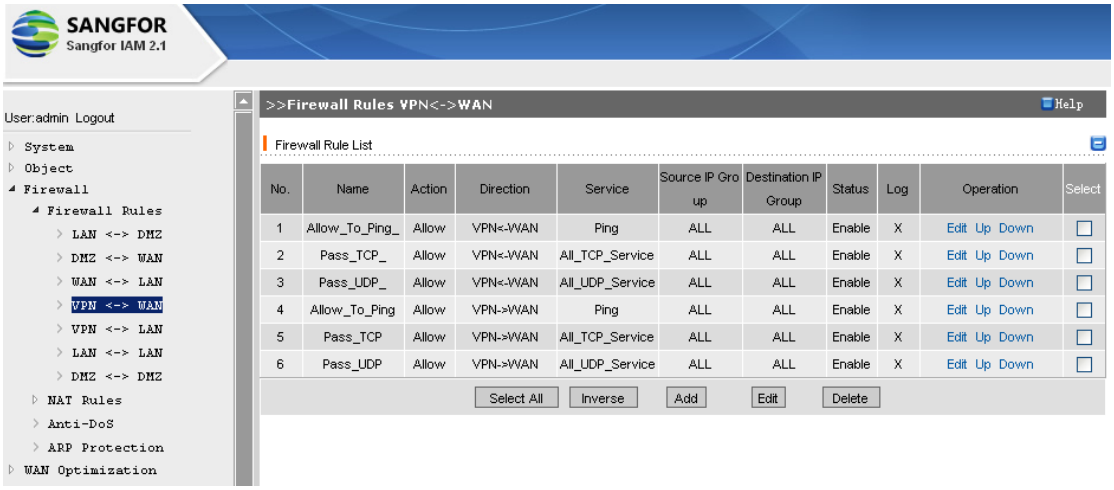
In the [Firewall Rule List], information of [Service], [Source IP Group], [Destination IP Group] can be configured in the corresponding page of [Object] or you can click the <Add> button followed to create a new one. For detailed configuration of each object, please refer to the corresponding section in Chapter 4 Object.

[WAN<->LAN] is a most common firewall rule. The IAM gateway device has some built-in and frequently-used firewall rules which default to let pass all the data packets from the external networks.

5.1.4. VPN <-> WAN

[VPN<->WAN] configures the firewall filtering rule for data transmission fulfilled between the VPN interface and WAN interface. If the VPN client connects to the headquarters' VPN device and gets access to the Internet through it, you then can configure the filtering rule of [VPN<->WAN] on the headquarters' VPN device to control the Internet access request sent from the client terminal (branch VPN user or mobile VPN user).

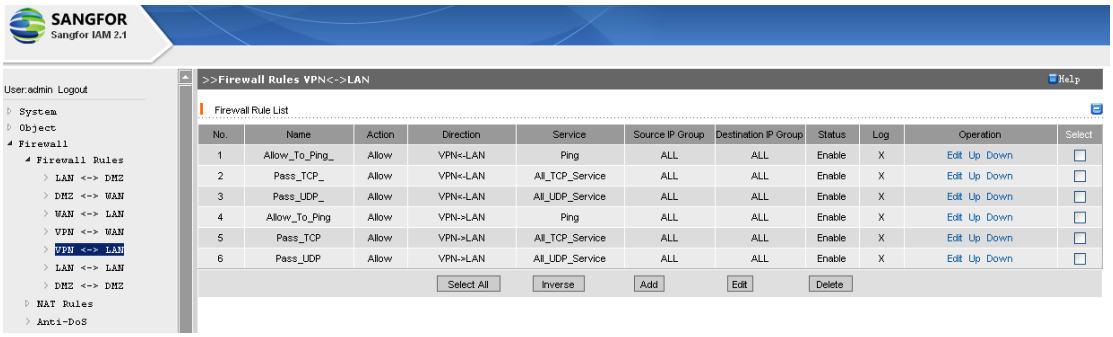
The configuration page is as shown below:



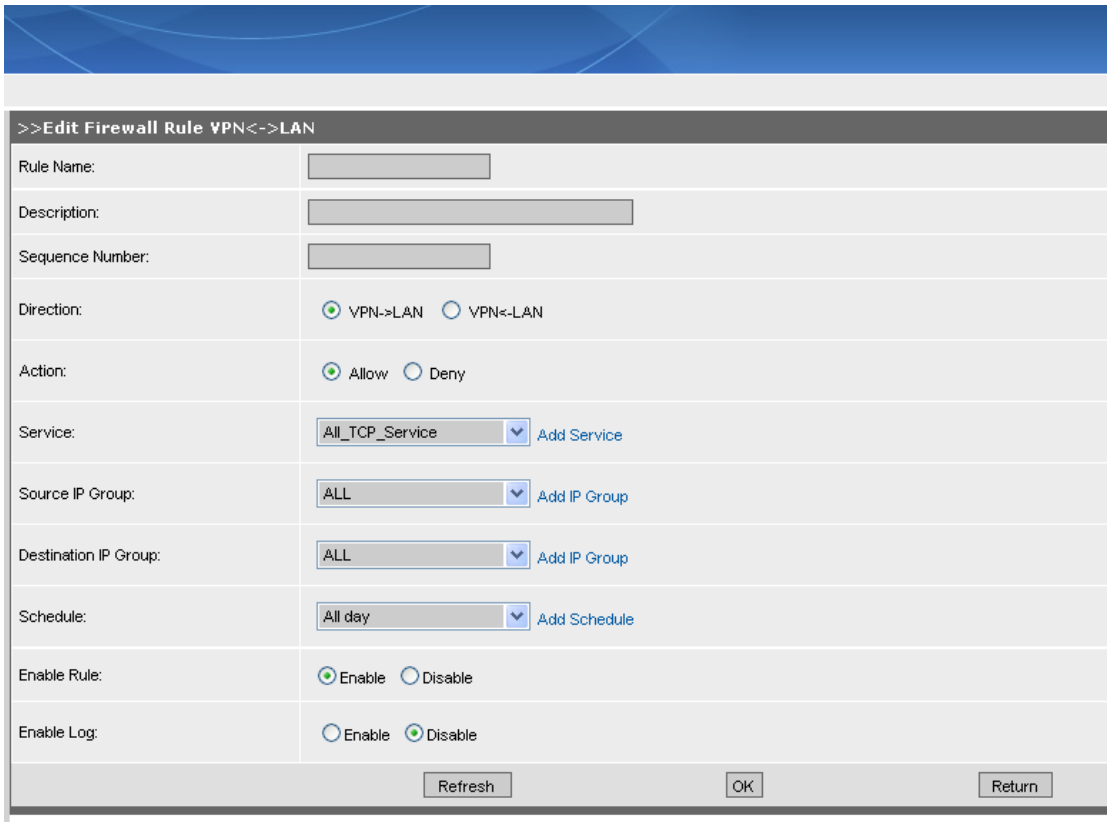
5.1.5. VPN<->LAN

[VPN<->LAN] configures the rule for data transmission between the VPN interface and the DMZ interface. By default, TCP, UDP and ICMP data transmission of both directions between the interfaces are allowed.

The configuration page is as shown below:



For instance, to allow the IP addresses (172.16.1.100-172.16.1.200) of a Branch VPN (172.16.0.0/24) to get access to the WEB server (192.168.1.20) of the headquarters and ban it from accessing to the SQL SERVER, you need first to create a filtering rule on WEB server. Detailed configuration is shown in the following figure:

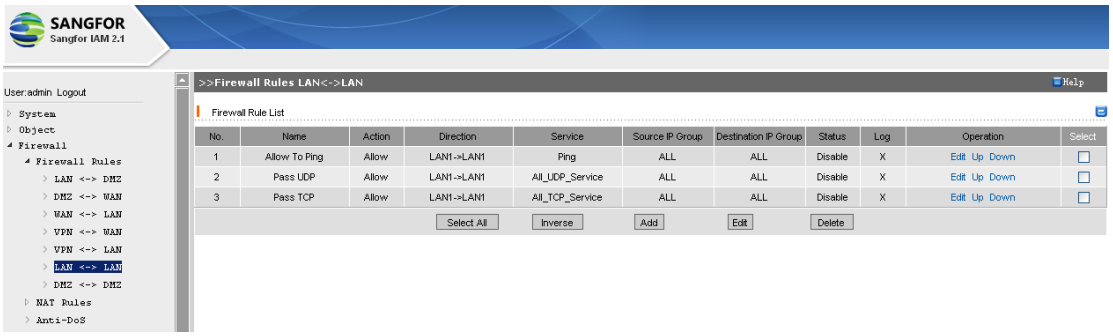


As to other kinds of data packets from the VPN headquarters or the Branch VPN, you can also configure filtering rule(s) for the data transmission between other interfaces.

5.1.6. LAN<->LAN

[LAN <-> LAN] configures the data transmission between the LAN1 interface (LAN interface on the IAM gateway device) and the LAN2 interface (the idle WAN2 interface on the IAM gateway device), or configures the communication among the IP addresses (of different segments) that are bound with the LAN interface. The service can be all the services of certain protocol or a user-defined service. For detailed configurations, please refer to Section 5.1.1 LAN <-> DMZ.

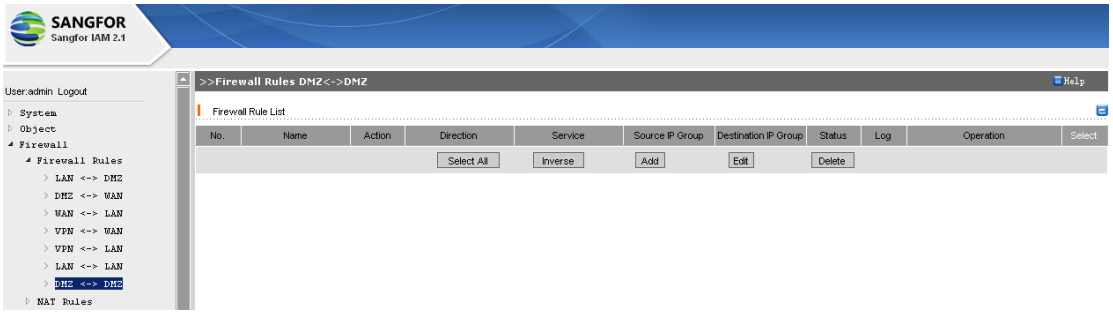
The default configuration page is as shown below:



5.1.7. DMZ <-> DMZ

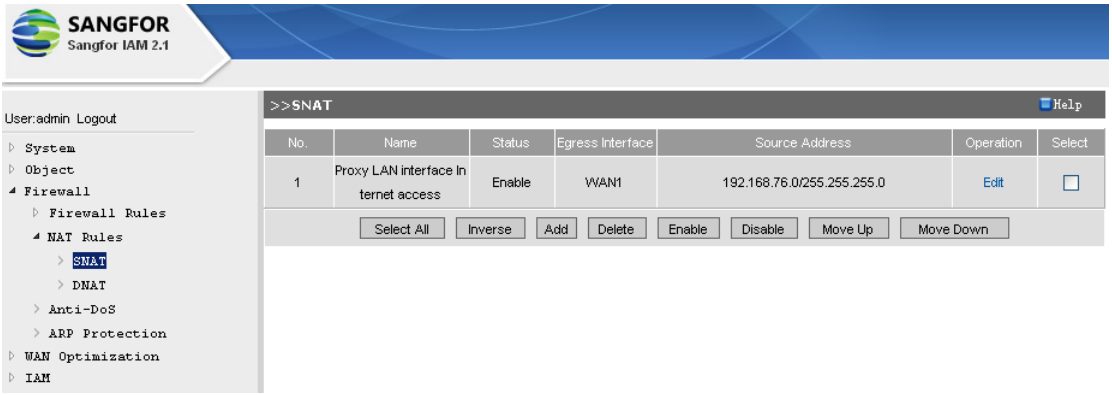
[DMZ <-> DMZ] configures the data transmission between the DMZ1 interface (DMZ interface on the IAM gateway device) and the DMZ2 interface (the WAN2 interface on the IAM gateway device), or configures the communication among the IP addresses (of different segment) that are bound with the DMZ interface. The service can be all the services of certain protocol or a user-defined service. For detailed configurations, please refer to Section 5.1.1 LAN <-> DMZ.

The default configuration page is as shown below:



5.2. NAT Rules

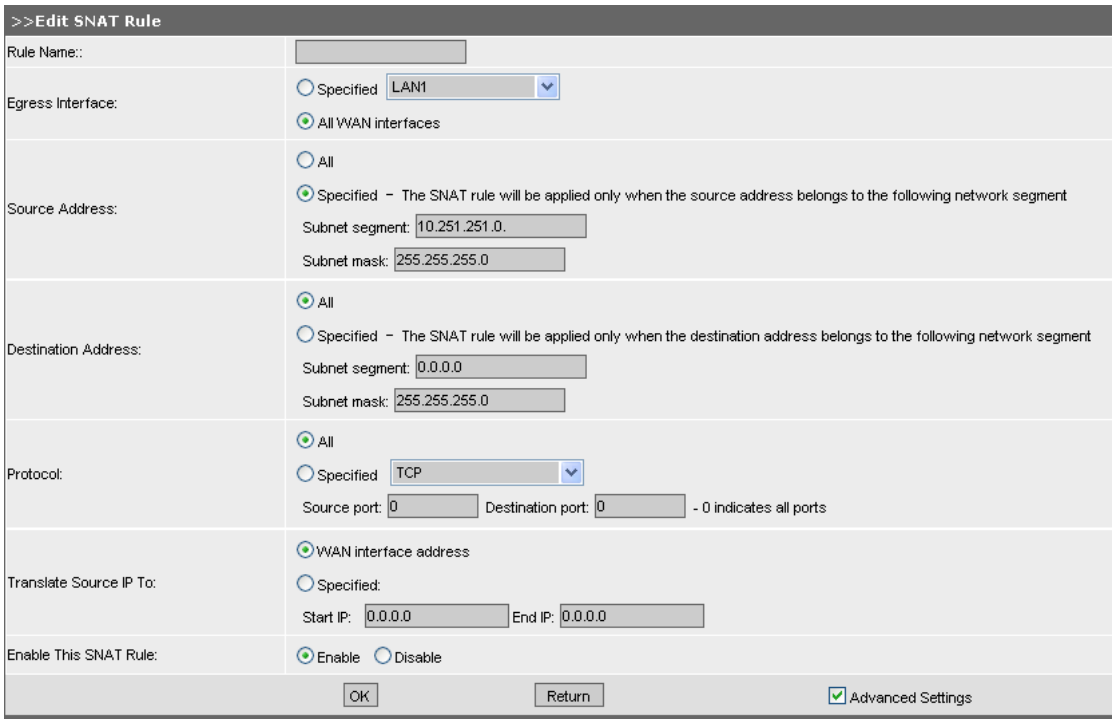
[NAT Rules] covers [SNAT] and [DNAT] configurations. The default configuration page is as shown below:



5.2.1. SNAT

Provided that a LAN IP address is 192.168.1.0./255.255.255.0, to create a SNAT (source network address translation) rule to proxy all the LAN users to get access to the Internet, you need to configure the followings.

Under the default configuration page of [SNAT Rules], click the <Add> button to enter the [Edit SNAT Rule], as shown below:



Type in a [Rule Name] to name this rule.

Select an [Egress Interface], a specified network interface or select [All WAN interfaces] to which the data packets are forwarded to.

Select [Source Address], [All] the IP addresses or a [Specified] subnet, which can get access to the Internet through the IAM gateway. In this example, the configured source address is the subnet 10.251.251.0/255.255.255.0.

Configure [Translate Source IP to], [WAN interface address] or [Specified] IP addresses. [Specified] requires [Start IP] and [End IP] (they are only required while the IP address and line is specified for Internet access). Generally, we select [WAN interface address] which means the source address can access all the public IP addresses through the WAN interface(s).

If [Advanced Settings] is checked, more settings are seen. Detailed introductions are as follows:

[Destination Address]: Options are [All] and [Specified]. [All] means all the destination IP addresses, while [Specified] indicates that the destination addresses are the specified ones.

[Destination Address] and [Source Address] can be configured at the same time. If both of them are configured, only when both of the conditions are satisfied will the source translation (SNAT) rule will be fulfilled; if only one of the conditions is configured, then only the corresponding condition needs to be satisfied.

[Protocol]: Options are [All] and [Specified]. [All] indicates all the protocol on which the SNAT rule is applied; [Specified] is selected and entered when the protocol and line applied are specified.

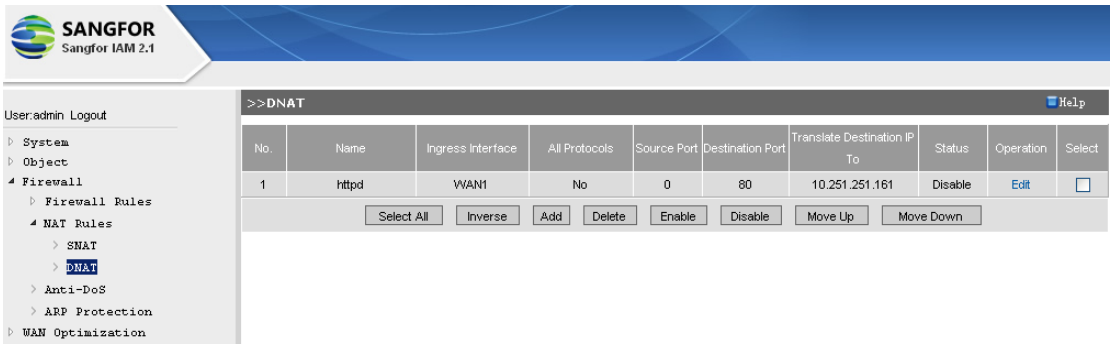
Having completed configuring this page, you have to click the <OK> button to save the settings.

Firewall rule [LAN->WAN] has to be configured to allow the data transmission.

5.2.2. DNAT

If a LAN (local area network) server needs to provide Internet with services, the [DNAT] function of IAM gateway device has to be configured.

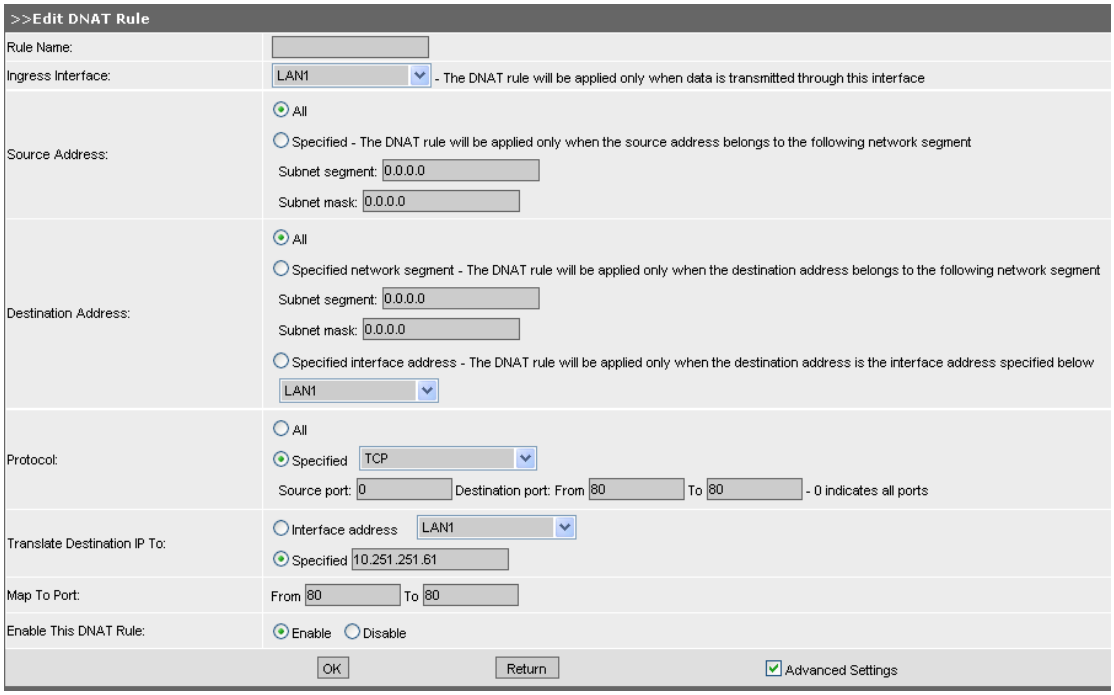
The default configuration page of [DNAT] rule is as shown below:



Provided that a LAN PC (IP address: 10.251.251.61) wants to provide the external network with WEB services, at port 80, follow the procedures below to configure a DNAT rule:

Under the [DNAT] configuration page, click the <Add> button to enter the [Edit DNAT Rule]

page, as shown below:


>>Edit DNAT Rule
Rule Name:
Ingress Interface:
LAN1
- The DNAT rule will be applied only when data is transmitted through this interface
Source Address:
All
Specified - The DNAT rule will be applied only when the source address belongs to the following network segment
Subnet segment: 0.0.0.0
Subnet mask: 0.0.0.0
Destination Address:
All
Specified network segment - The DNAT rule will be applied only when the destination address belongs to the following network segment
Subnet segment: 0.0.0.0
Subnet mask: 0.0.0.0
Specified interface address - The DNAT rule will be applied only when the destination address is the interface address specified below
LAN1
Protocol:
All
Specified
TCP
Source port: 0
Destination port: From 80 To 80
- 0 indicates all ports
Translate Destination IP To:
Interface address
LAN1
Specified
10.251.251.61
Map To Port:
From 80 To 80
Enable This DNAT Rule:
Enable
Disable
OK
Return
Advanced Settings

Type a [Rule Name] to name this DNAT rule;

Select an [Ingress Interface];

Select a [Protocol], [All] the protocols or the [Specified] protocol TCP; enter [Source port] 0 (indicates all the ports), [Destination port] 80~80;

Enter the [Translate Destination IP To] 10.251.251.61;

Enter the [Map To Port] 80~80.

If [Advanced Settings] is checked, more settings are seen. Detailed introductions are as follows:

[Source Address]: Options are [All] and [Specified]. [All] means all the source IP addresses, while [Specified] indicates that the source addresses are the specified ones.

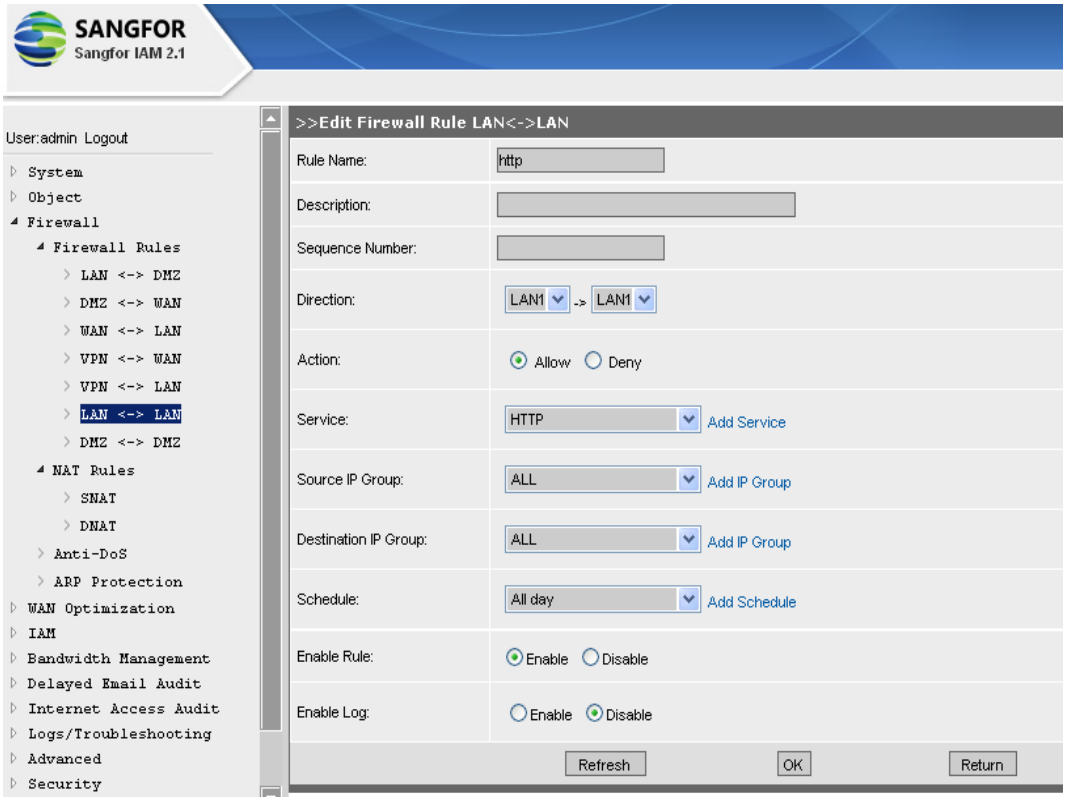
[Destination Address]: Generally, [Specified interface address] is selected. If the WAN interface has several IP addresses, you can select the [Specified network segment] to specify the WAN interface IP address or IP range which are then be translated to the IP address of the local area network.

[Destination Address] and [Source Address] can be configured at the same time. If both of them are configured, only when both of the conditions are satisfied will the SNAT rule will be fulfilled; if only one of the conditions is configured, then only the corresponding condition needs to be

satisfied.

Having completed configuring this page, you have to click the <OK> button to save the settings.

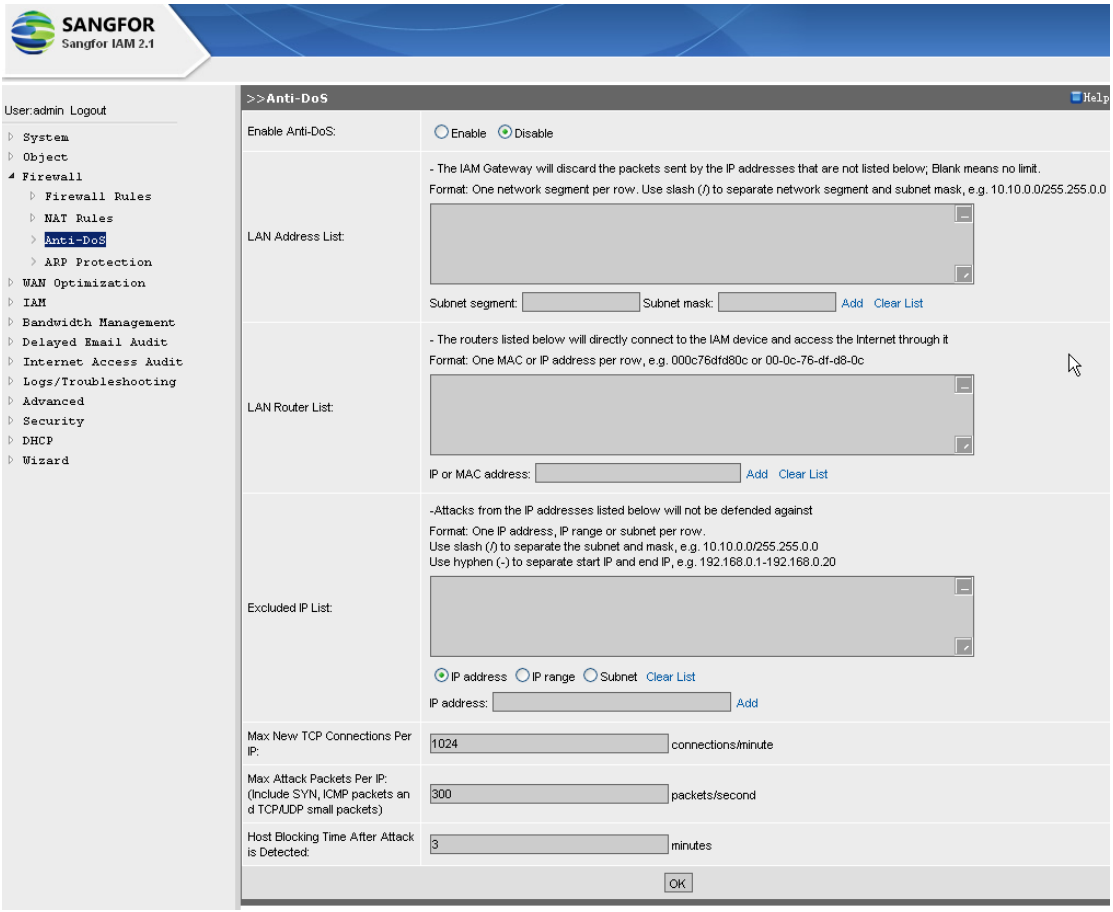
- If the [Source port] of TCP [Protocol] is configured as 0, it indicates all the ports.
- Settings of allowing any Internet IP address to access the LAN IP 10.251.251.61 at port 80 are configured in [Firewall] > [Firewall Rules] > [WAN<->LAN] page. For details, please refer to Section 5.1.3 WAN<->LAN. The configuration page is as shown below:



5.3. Anti-DoS

DoS attack (Denial of Service attack), generally is implemented by forcing the server to reset or saturating the server with external communication requests and consuming its resources, so that it can no longer provide intended service and respond to legitimate computers. SANGFPR IAM gateway device can defend the local area network against DoS attacks from external networks, and take measures to prevent the infected machine or attack tool from initiating DoS attacks. It can locate the attack source with the IP and MAC information

The configuration page is shown below:



[Enable Anti-DoS]: Select [Enable] to enable the anti-DoS function.

[LAN Address List]: Configures the LAN IP range which gets access to the Internet through the SANGFOR IAM gateway device. The data packets from the IP addresses outside the [LAN Address List] will be dropped by the IAM gateway device, which means these blocked IP addresses will fail to connect to the Internet through the IAM gateway device or connect to the IAM gateway device through LAN and DMZ interface (mistakes made on this list may result in login failure to the console through the LAN interface; in that case, log in through the WAN interface). The [LAN Address List] can be left blank, but configuring it will enable the SANGFOR IAM gateway device to defend against DoS attacks, such as attacks by masqueraded IP address.

[LAN Router List]: Configures the router (without enabling NAT function) or layer 3 switch that connects to the LAN interface or DMZ interface of the IAM gateway device. If a PC is not at the same segment of the LAN interface or DMZ interface of the IAM gateway device, the MAC address of this PC will be replaced by the MAC address of the routing device. In case the number of connections of this routing device is more than expected, the routing device's interface (at the

same segment with IAM gateway device) will be blocked by the IAM gateway device. This [LAN Router List] will prevent the MAC address of the LAN router (in the list) from being blocked by the IAM gateway device.

You can enter interface IP address or MAC address of the router (or layer 3 switch) that directly connects to the LAN interface of the IAM gateway device. The IAM gateway device will automatically distinguish the MAC address of the corresponding IP address.

[Excluded IP List]: Configures the IP address(es) that will not be defended against in any case, regardless of the number of connections and high frequency of sending packets. Generally, the connections and frequency of sending packet of an IP address is limited; if any of the standards is reached, it will be regarded as DoS attack.

[Max New TCP Connections Per IP]: Configures the maximum TCP connections of each IP allowed by the IAM gateway device in one minute. If number of new TCP connections of an IP address exceeds the limit configured herein, the IP will be blocked for a certain time ([Host Blocking Time After Attack is Detected]).

[Max Attack Packets Per IP]: Configures the maximum packets (including SYN packets, ICMP packets and TCP/UDP small attack packets) of each IP or MAC address allowed by the IAM gateway device in one second. If number of them exceeds the limit configured herein, the IP or MAC address will be blocked for a certain time ([Host Blocking Time After Attack is Detected]).

[Host Blocking Time After Attack is Detected]: Configures the time duration of blocking the host if the IAM gateway device detects that this host is initiating attacks; in unit of minutes.

- It is strongly recommended to enable the anti-DoS function, which will enable the IAM gateway device to efficiently defend attacks initiated by external networks and to prevent traffic congestion caused by enormous and continuous packets that are sent by the virus-infected LAN PC.
- [LAN Address List] is also recommended to be configured. This configuration will help to defend against attacks initiated by masqueraded IP address. Better to add all the LAN segments to the list, for the data packets sent by the IP addresses outside the list will be then forwarded to the IAM gateway device and then be dropped.
- If there is a LAN router or layer 3 switch, please DO add the routing device's interface IP

(that directly connects to the IAM gateway device) to the [LAN Router List], so that the MAC address of this interface is excluded from the anti-DoS rule and from being blocked. Generally, if the WAN interface of the IAM gateway device connects to any firewall or router, the interface IP address of this routing device should be added into the [LAN Router List].

- By default, the [Max New TCP Connections Per IP] in one minute of an IAM gateway device anti-DoS module is 1024, and the [Max Attack Packets Per IP] is 300. If the local area network is virus-infected and sending enormous packets, resulting in disconnection of the network, it is recommended to modify [Max New TCP Connections Per IP] to 512 and [Max Attack Packets Per IP] to a smaller value, and then the defense against the LAN virus-infected computers can be more efficient.
- As the download software Thunder allows massive connections, and thus features like DoS attack. Because of this feature, the IAM gateway device may block the LAN PC that is running Thunder software. To solve this problem, you can set an appropriate value to lower the possibility the computer being blocked by the IAM gateway device. Configure the [Max New TCP Connections Per IP] as 1024 connections/minute and [Max Attack Packets Per IP] as 512 packets/second.

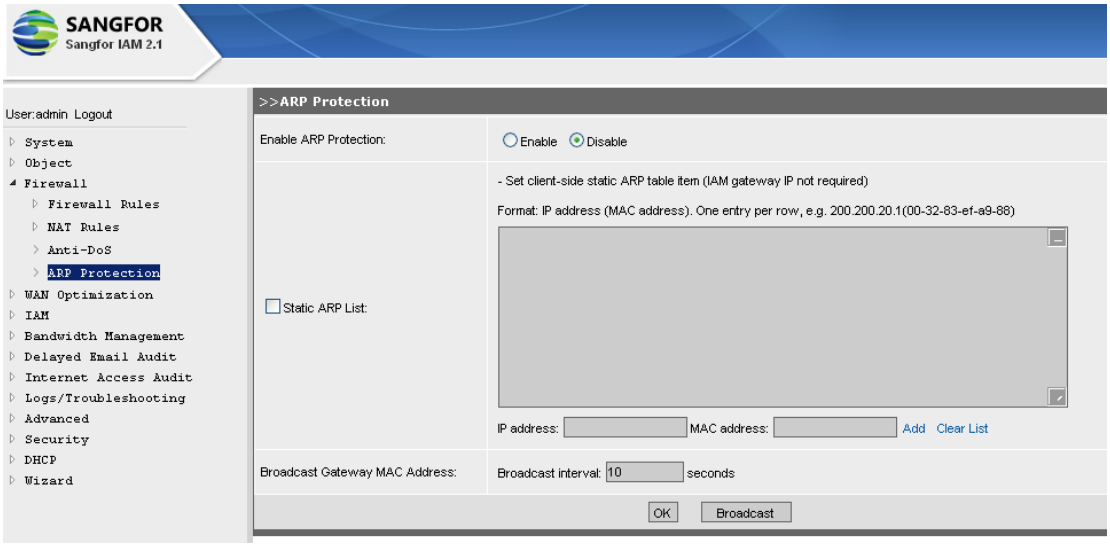
5.4. ARP Protection

ARP spoofing is a common LAN virus. The infected computer keeps sending fake (or spoofed) message (broadcast packets) to the local area network (LAN), and thus interrupts and stops the normal communication among the LAN devices, or even stops the overall traffic of the local area network.

Defense against ARP spoofing is fulfilled through the ARP protection function of IAM gateway device in association with the Ingress Client installed in the LAN PC. After installing the Ingress Client, the Ingress Client will communicate with the IAM gateway device to get the correct IP/MAC information of the gateway device and bind with it. The IAM gateway device will refuse to receive the ARP request or response that features attack, so as to protect the ARP cache of the local IAM gateway device and get immune from ARP spoofing.

However, if the user related to access control policy is bound with an IP/MAC address(es), the IAM gateway device will take the bound ones (in [Organization Structure] > [Edit User] page > [Advanced Settings] > [User Attribute]) as the final IP/MAC address(es).

The configuration page is as shown below.



[Enable ARP Protection]: Select [Enable] to enable the ARP spoofing protection function.

[Static ARP List]: If the gateway of the LAN PC is not an interface IP address of the IAM gateway device, the [Static ARP List] should be configured. Provided that, the gateway mode of the IAM gateway device is Bridge mode; the gateway address of the LAN PC is the interface IP address of its front-end router (or firewall), in this case, we have to add the IP/MAC address of the front-end router to the [Static ARP List]. If the LAN PC has installed the Ingress Client, then it can get the correct IP/MAC address of the gateway and bind with it; therefore, we can make sure that the IP/MAC address of the gateway is correct.

[Broadcast Gateway MAC Address]: Indicates the frequency broadcasting the MAC address of the gateway (the LAN interface of the IAM gateway device), in unit of second.

<Broadcast>: Click this button to manually and immediately broadcast the MAC address of the device's LAN interface. When the ARP spoofing is eliminated, clicking this button can restore the ARP table of the LAN PC swiftly.

Having completed configuring this page, you have to click the <OK> button to save the settings.

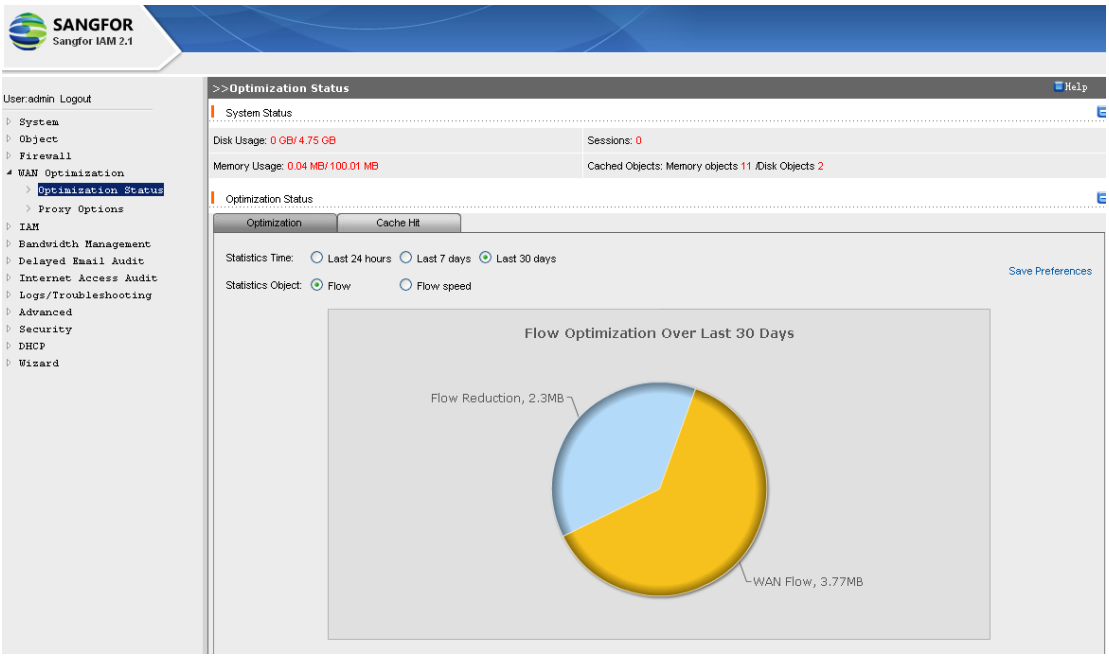
Chapter 6 WAN Optimization

In a real enterprise network, the bandwidth resources are limited and bandwidth resources waste also exists. It is possible that thousands of LAN users visit a well-known website and the same data have to be transmitted thousands of times or more, which consumes and wastes massive bandwidth resources.

The SANGFOR IAM gateway device will help to solve this problem. The preliminary data requested by a LAN user who visits this website for the first time will be cached by the IAM gateway device, if a second LAN user wants to visit the same website, the requested data (basically the same with the data requested by the first LAN user) will be directly fetched from the cache; the user need not request data resources over the Internet.

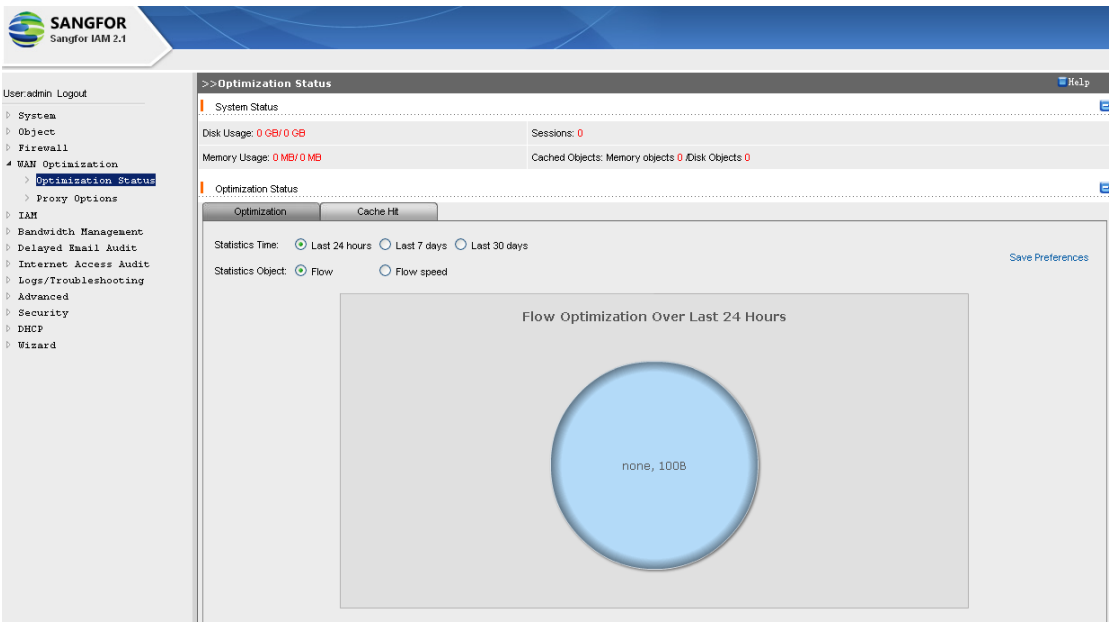
[WAN Optimization] covers [Optimization Status] and [Proxy Options]. The cache function can accelerate HTTP application and improve the speed of visiting websites.

The default page is as shown below:



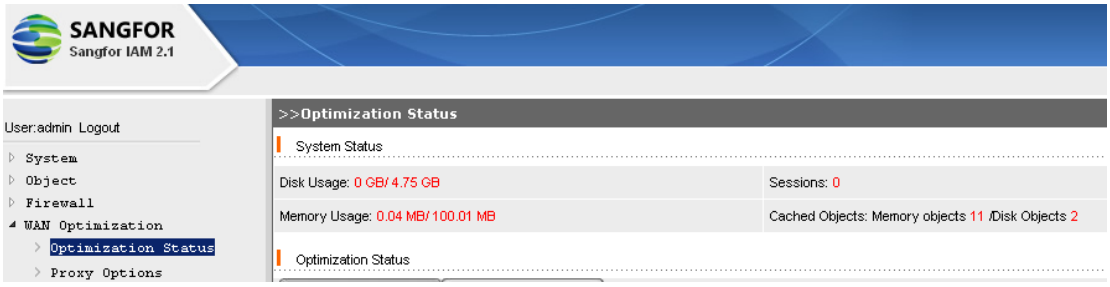
6.1. Optimization Status

[Optimization Status] displays the cache and optimization (acceleration) information, including [System Status] and [Optimization Status] modules, as shown below:



6.1.1. System Status

[System Status] displays the disk usage, sessions, memory usage and cached objects information, as shown below:



[Disk Usage]: Displays the utilized disk space by and the available disk space for optimization.

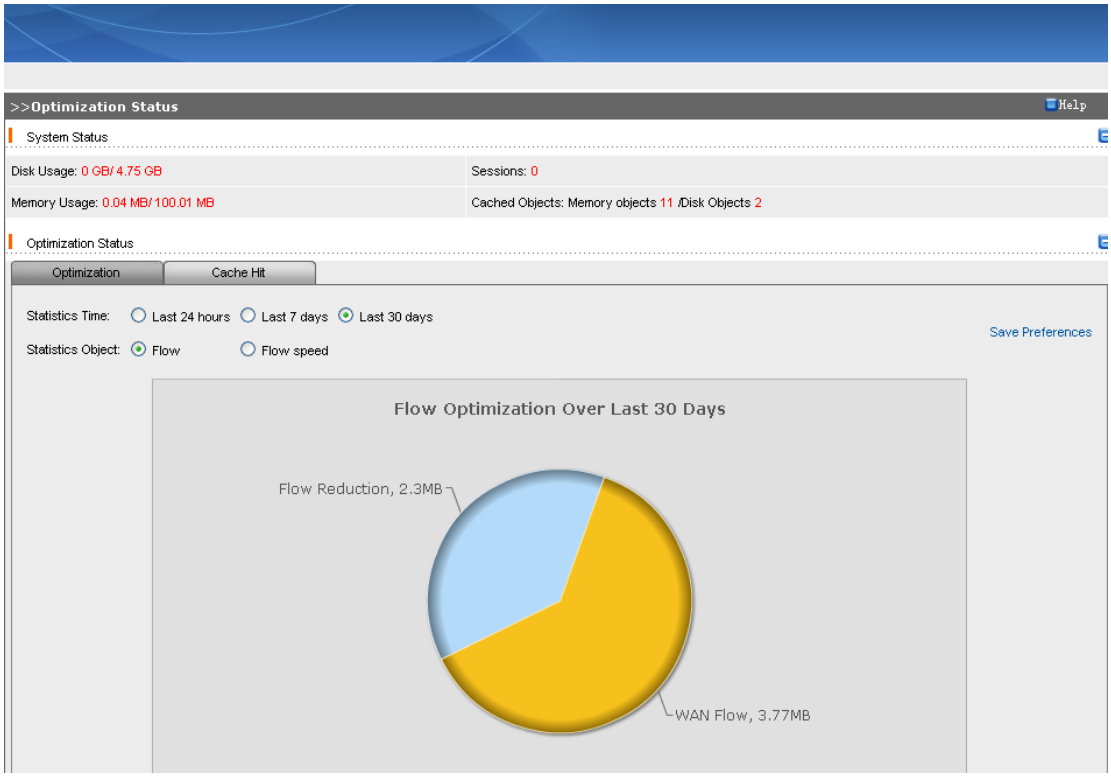
[Sessions]: Refreshes and displays the total current sessions every five minutes.

[Memory Usage]: Displays the utilized memory by and the maximum available memory space for optimization.

[Cached Objects]: Displays the total cached objects in the memory and the total objects in the disk.

6.1.2. Optimization Status

[Optimization Status] displays the [Optimization] and [Cache Hit] information, as shown below:

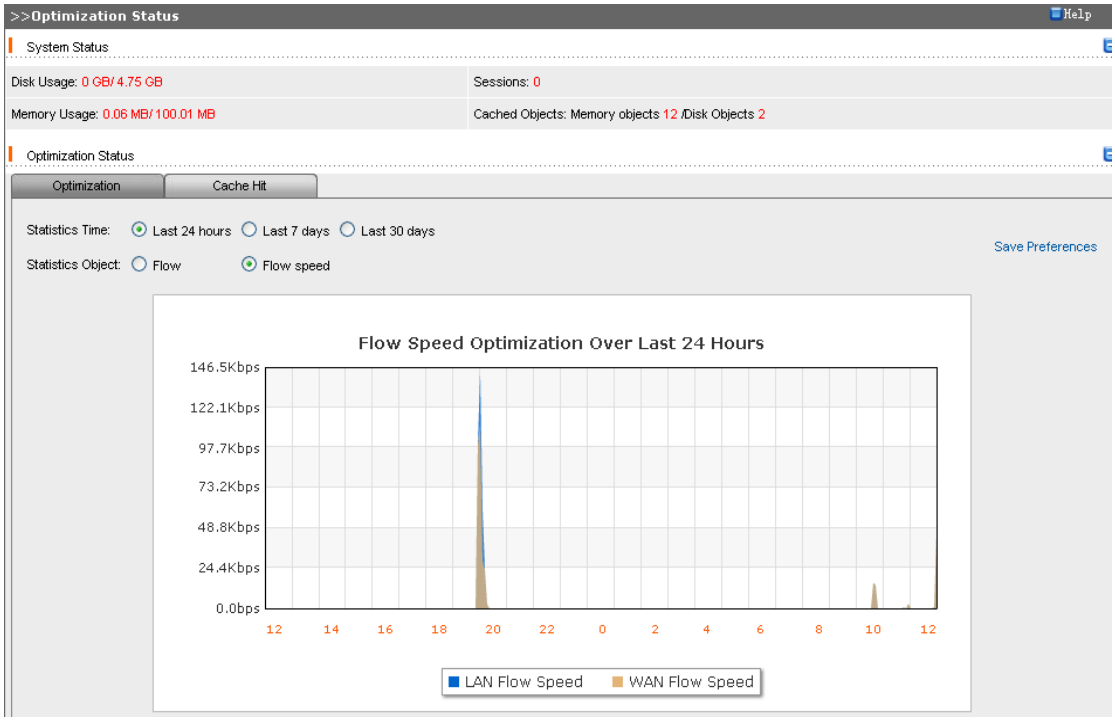


[Optimization] displays two kinds of statistics objects, one is [Flow], and the other is [Flow Speed], in time unit of [Last 24 hours], [Last 7 days] or [Last 30 days].

[Flow]: Makes statistics of traffic volume passing through and the traffic volume saved by the WAN optimization module. The saved traffic volume indicates the data (cached in the IAM gateway device) being matched by the sequential visits to the extranet server, that is, volume of the data request directly responded by the IAM gateway device. This part of traffic volume shows the external bandwidth saved by the IAM gateway device.

[Flow speed]: Displays the flow speed of the data that are passing through the IAM WAN optimization module. The information is displayed on rectangular coordinates, X axis in unit of time and Y axis in unit of flow speed.

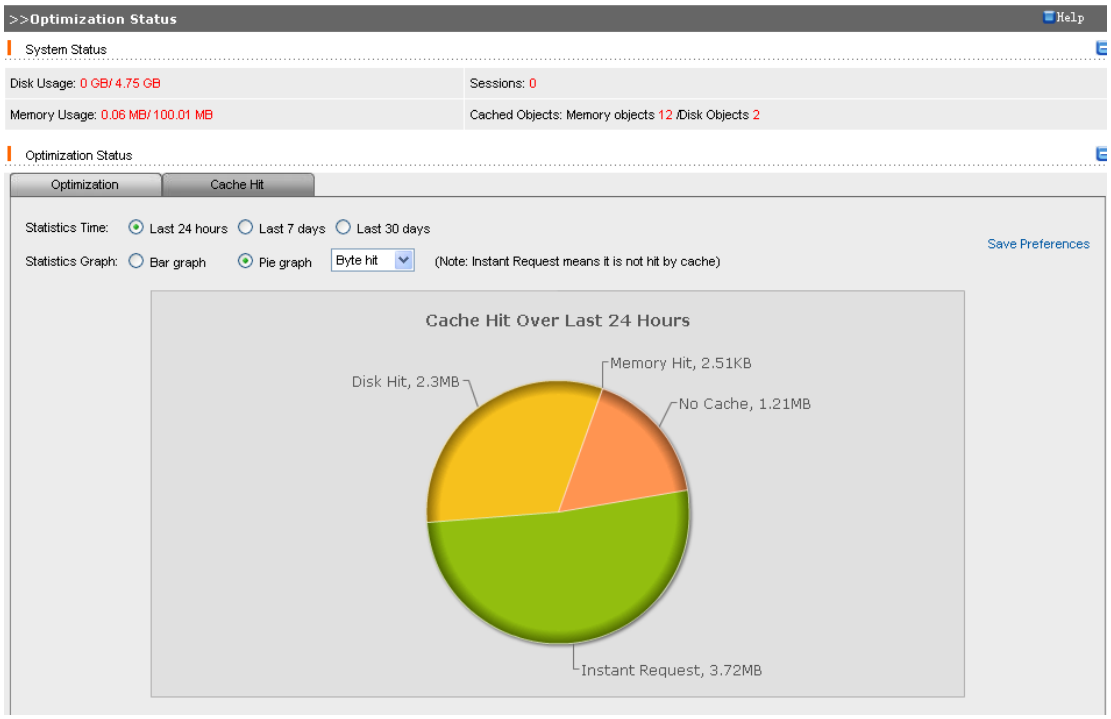
Flow speed are [LAN Flow Speed] and [WAN Flow Speed]. [LAN Flow Speed] means the flow speed the IAM gateway device directly responded to the LAN user's website access requests. These portions of data do not reach the public network, and thus consumes no public bandwidth. [WAN Flow Speed] means the flow speed of the data that the IAM gateway device forwarded to the extranet server plus that of the extranet network giving response to the LAN user's request.



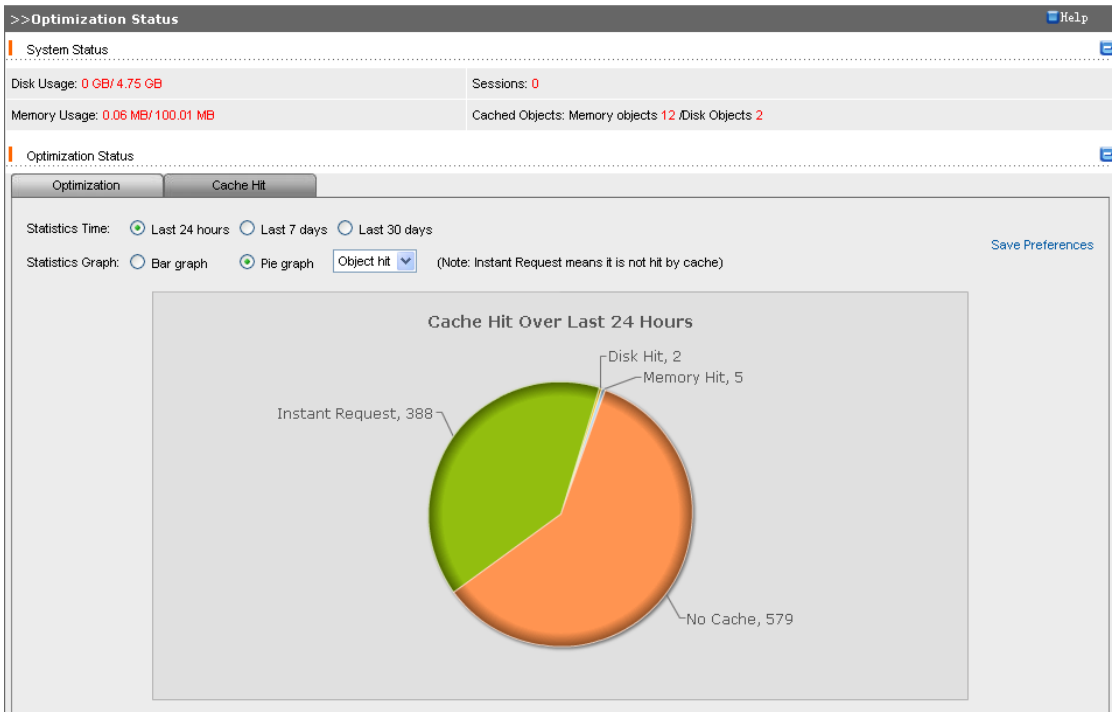
6.1.3. Cache Hit

[Cache Hit] makes statistics of the percentage and times the cached data being matched (hit) by the requested data. The information is displayed in [Bar graph] and [Pie graph]. Hits may be counted by object or by byte; [Byte hit] indicates the cached hit percent or traffic volume on flow.

The [Pie graph] on [Byte hit] is as shown below:


>>Optimization Status
Help
System Status
Disk Usage: 0 GB/ 4.75 GB
Sessions: 0
Memory Usage: 0.06 MB/ 100.01 MB
Cached Objects: Memory objects 12 /Disk Objects 2
Optimization Status
Optimization
Cache Hit
Statistics Time: Last 24 hours Last 7 days Last 30 days
Statistics Graph: Bar graph Pie graph Byte hit
(Note: Instant Request means it is not hit by cache)
Save Preferences
Cache Hit Over Last 24 Hours
Memory Hit, 2.51KB
Disk Hit, 2.3MB
No Cache, 1.21MB
Instant Request, 3.72MB

The [Pie graph] on [Object hit] is as shown below:


>>Optimization Status
Help
System Status
Disk Usage: 0 GB/ 4.75 GB
Sessions: 0
Memory Usage: 0.06 MB/ 100.01 MB
Cached Objects: Memory objects 12 /Disk Objects 2
Optimization Status
Optimization
Cache Hit
Statistics Time: Last 24 hours Last 7 days Last 30 days
Statistics Graph: Bar graph Pie graph Object hit (Note: Instant Request means it is not hit by cache)
Save Preferences
Cache Hit Over Last 24 Hours
Disk Hit, 2
Memory Hit, 5
Instant Request, 388
No Cache, 579

[Memory Hit]: Indicates the cached data (in the memory of the IAM gateway device) being hit by the LAN-user-requested data and being accelerated.

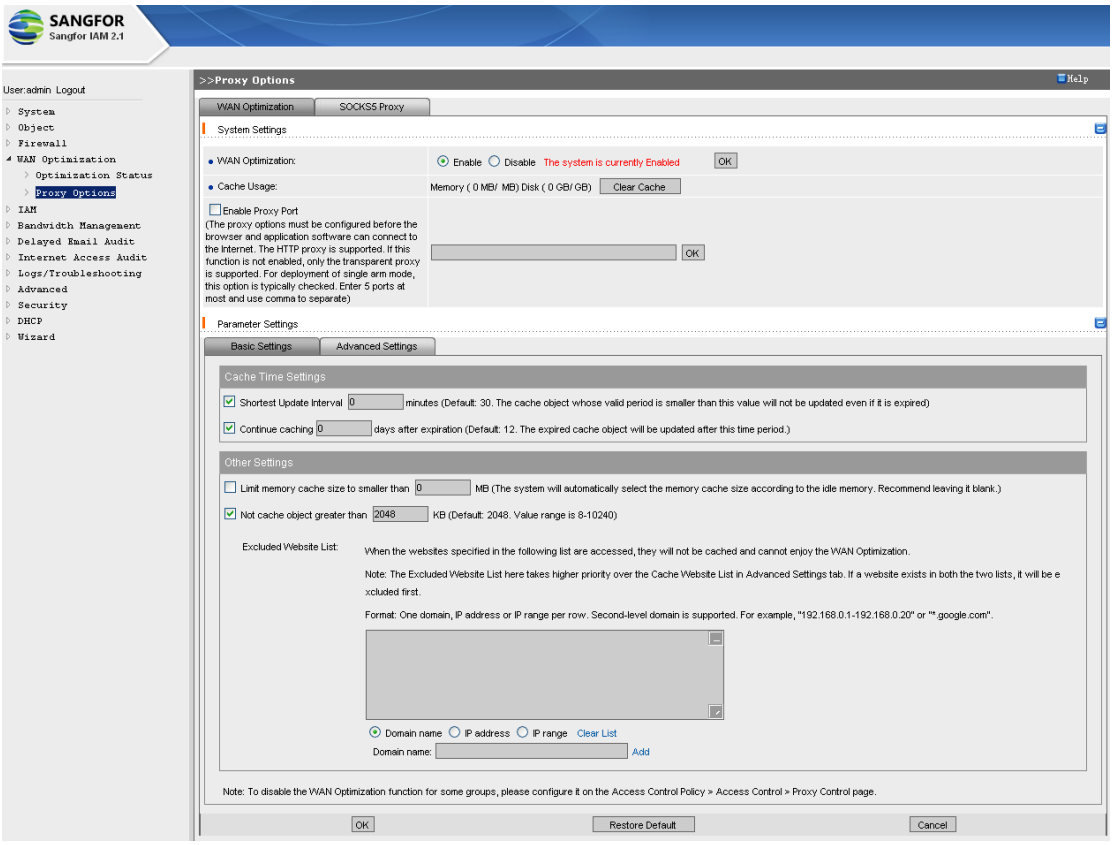
[Disk Hit]: Indicates the cached data (in the disk of the IAM gateway device) being hit by the LAN-user-requested data and being accelerated.

[Instant Request]: Indicates the data requested by the LAN user for the first time or the request data that are not hit by the cached data.

[No Cache]: Indicates the requested data that the extranet server claims not allowed to be cached or the browser of the LAN user claims not allowed to be cached, and indicates the object that is larger than the object size limit configured in [WAN Optimization] > [Proxy Options] page > [WAN Optimization] > [Basic Settings] > [Other Settings].

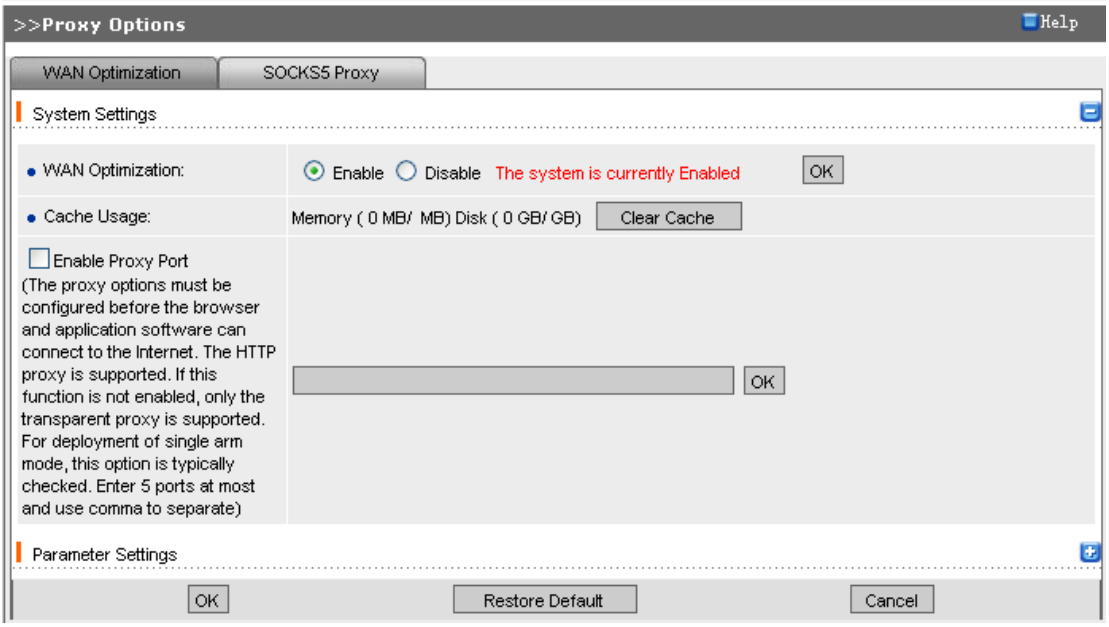
6.2. Proxy Options

[Proxy Options] covers [System Settings] and [Parameter Settings], as shown below:


SANGFOR
Sangfor IAM 2.1
User:admin Logout
System
Object
Firewall
WAN Optimization
Optimization Status
Proxy Options
IAM
Bandwidth Management
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Security
DHCP
Wizard
>>Proxy Options
Help
WAN Optimization
SOCKS5 Proxy
System Settings
WAN Optimization:
Enable
Disable
The system is currently Enabled
OK
Cache Usage:
Memory (0 MB/ MB) Disk (0 GB/ GB)
Clear Cache
Enable Proxy Port
(The proxy options must be configured before the browser and application software can connect to the Internet. The HTTP proxy is supported. If this function is not enabled, only the transparent proxy is supported. For deployment of single arm mode, this option is typically checked. Enter 5 ports at most and use comma to separate)
OK
Parameter Settings
Basic Settings
Advanced Settings
Cache Time Settings
Shortest Update Interval 0 minutes (Default: 30. The cache object whose valid period is smaller than this value will not be updated even if it is expired)
Continue caching 0 days after expiration (Default: 12. The expired cache object will be updated after this time period.)
Other Settings
Limit memory cache size to smaller than 0 MB (The system will automatically select the memory cache size according to the idle memory. Recommend leaving it blank.)
Not cache object greater than 2048 KB (Default: 2048. Value range is 8-10240)
Excluded Website List:
When the websites specified in the following list are accessed, they will not be cached and cannot enjoy the WAN Optimization.
Note: The Excluded Website List here takes higher priority over the Cache Website List in Advanced Settings tab. If a website exists in both the two lists, it will be e xcluded first.
Format: One domain, IP address or IP range per row. Second-level domain is supported. For example, "192.168.0.1-192.168.0.20" or "*.google.com".
Domain name
IP address
IP range
Clear List
Domain name:
Add
Note: To disable the WAN Optimization function for some groups, please configure it on the Access Control Policy > Access Control > Proxy Control page.
OK
Restore Default
Cancel

6.2.1. System Settings

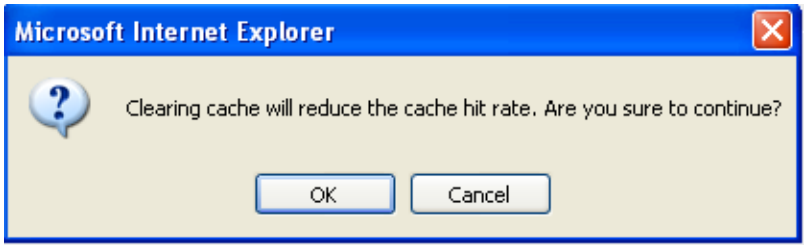
[System Settings] globally enables or disables the WAN optimization function, as well as displays the [Cache Usage] information. You can also clear the cache on this page.


>>Proxy Options
Help
WAN Optimization
SOCKS5 Proxy
System Settings
WAN Optimization:
Enable
Disable
The system is currently Enabled
OK
Cache Usage:
Memory (0 MB/ MB) Disk (0 GB/ GB)
Clear Cache
Enable Proxy Port
(The proxy options must be configured before the browser and application software can connect to the Internet. The HTTP proxy is supported. If this function is not enabled, only the transparent proxy is supported. For deployment of single arm mode, this option is typically checked. Enter 5 ports at most and use comma to separate)
OK
Parameter Settings
OK
Restore Default
Cancel

[WAN Optimization]: Globally enables the WAN optimization function. Select [Enable] or

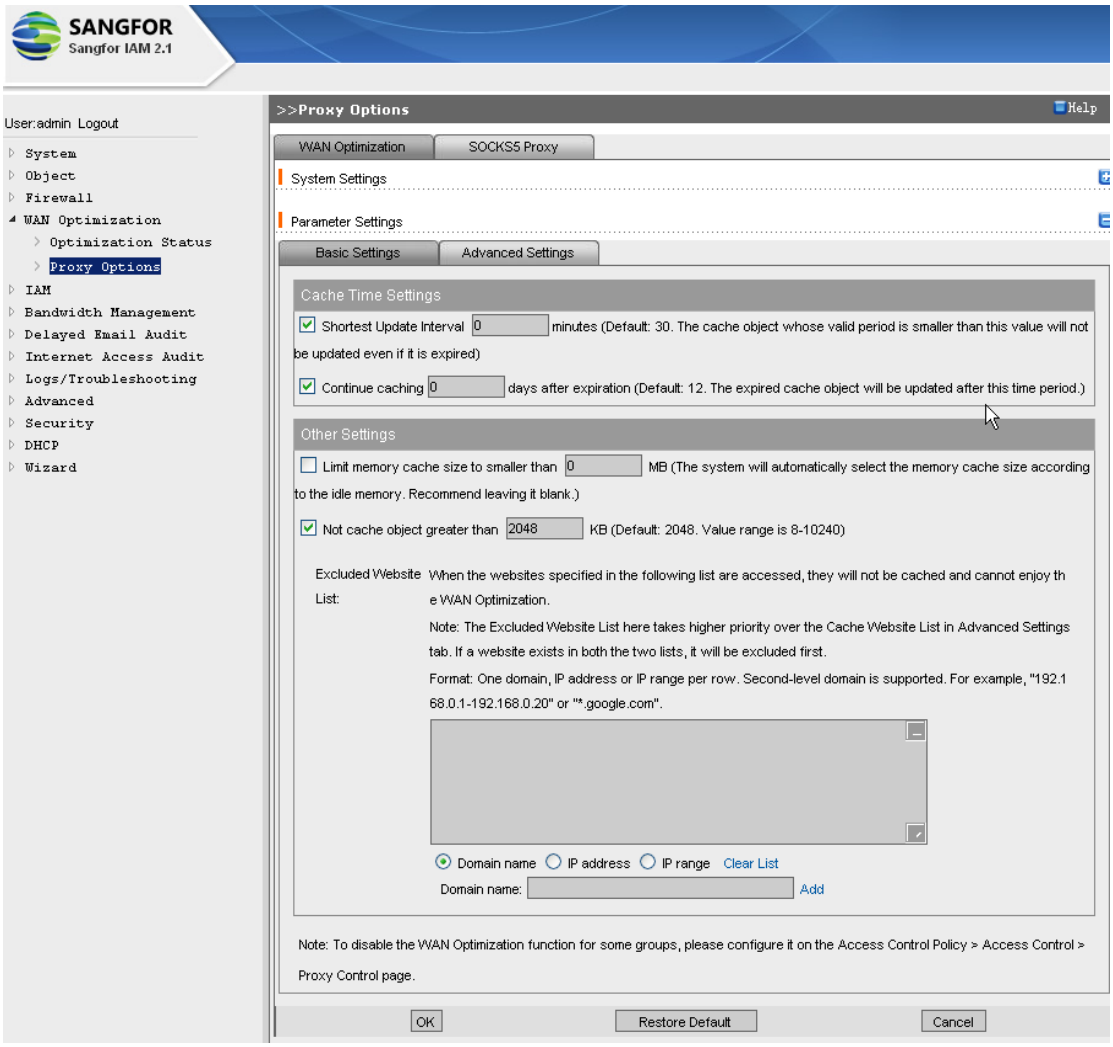
[Disable] and then click the <OK> button to enable and disable this module respectively.

[Cache Usage]: Displays the utilized/maximum memory space and disk space. Click the <Clear Cache> button and it prompts whether to continue the operation, as shown below:



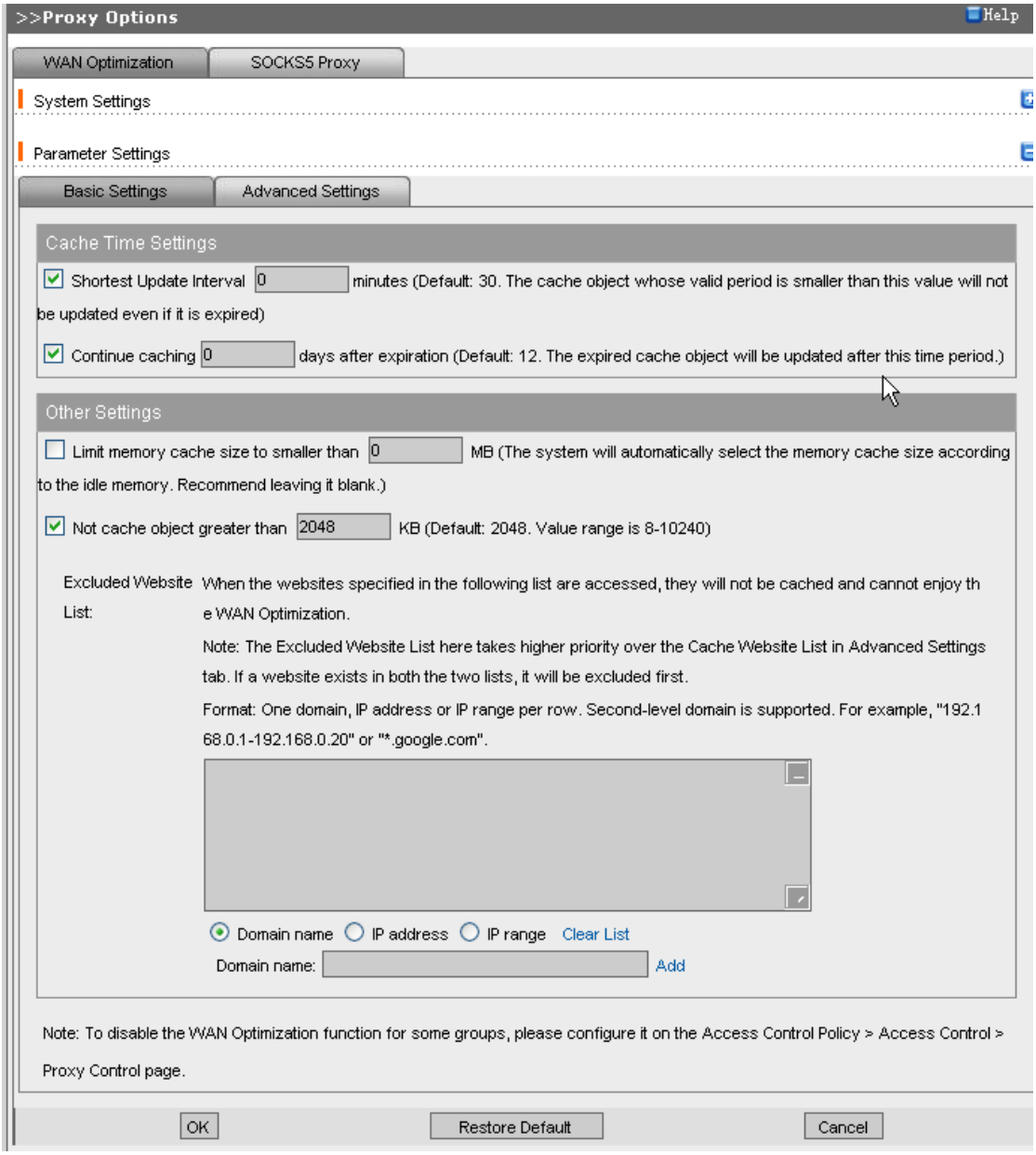
If you confirm to clear the cache, just click the <OK> button.

[Parameter Settings] covers [Basic Settings] and [Advanced Settings], as shown below:


SANGFOR
Sangfor IAM 2.1
User:admin Logout
System
Object
Firewall
WAN Optimization
Optimization Status
Proxy Options
IAM
Bandwidth Management
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Security
DHCP
Wizard
>>Proxy Options
Help
WAN Optimization
SOCKS5 Proxy
System Settings
Parameter Settings
Basic Settings
Advanced Settings
Cache Time Settings
Shortest Update Interval 0 minutes (Default: 30. The cache object whose valid period is smaller than this value will not be updated even if it is expired)
Continue caching 0 days after expiration (Default: 12. The expired cache object will be updated after this time period.)
Other Settings
Limit memory cache size to smaller than 0 MB (The system will automatically select the memory cache size according to the idle memory. Recommend leaving it blank.)
Not cache object greater than 2048 KB (Default: 2048. Value range is 8-10240)
Excluded Website List:
When the websites specified in the following list are accessed, they will not be cached and cannot enjoy the WAN Optimization.
Note: The Excluded Website List here takes higher priority over the Cache Website List in Advanced Settings tab. If a website exists in both the two lists, it will be excluded first.
Format: One domain, IP address or IP range per row. Second-level domain is supported. For example, "192.168.0.1-192.168.0.20" or "*.google.com".
Domain name
IP address
IP range
Clear List
Domain name:
Add
Note: To disable the WAN Optimization function for some groups, please configure it on the Access Control Policy > Access Control > Proxy Control page.
OK
Restore Default
Cancel

6.2.1.1. Basic Settings

[Basic Settings] includes [Cache Time Settings] and [Other Settings], as shown below:


>>Proxy Options
Help
WAN Optimization
SOCKS5 Proxy
System Settings
Parameter Settings
Basic Settings
Advanced Settings
Cache Time Settings
Shortest Update Interval 0 minutes (Default: 30. The cache object whose valid period is smaller than this value will not be updated even if it is expired)
Continue caching 0 days after expiration (Default: 12. The expired cache object will be updated after this time period.)
Other Settings
Limit memory cache size to smaller than 0 MB (The system will automatically select the memory cache size according to the idle memory. Recommend leaving it blank.)
Not cache object greater than 2048 KB (Default: 2048. Value range is 8-10240)
Excluded Website List:
When the websites specified in the following list are accessed, they will not be cached and cannot enjoy the WAN Optimization.
Note: The Excluded Website List here takes higher priority over the Cache Website List in Advanced Settings tab. If a website exists in both the two lists, it will be excluded first.
Format: One domain, IP address or IP range per row. Second-level domain is supported. For example, "192.168.0.1-192.168.0.20" or "*.google.com".
Domain name
IP address
IP range
Clear List
Domain name:
Add
Note: To disable the WAN Optimization function for some groups, please configure it on the Access Control Policy > Access Control > Proxy Control page.
OK
Restore Default
Cancel

[Shortest Update Interval: Check this option and configure the minimum interval the cache is updated by the IAM gateway device. The IAM gateway device will not update the cached objects within this time interval even though they have been updated by the server; only after this time interval will the IAM gateway device update the cached objects if there are new requests for it.

[Continue caching]: Check this item and configure the longest time the cached data will be cached. If it exceeds the time configured here, the corresponding cached data will be deleted to release disk space and memory space.

[Limit memory cache size to smaller than]: Check this item and configure the maximum value the memory can cache. The system will automatically adjust this value; it is not recommended to be altered manually.

[Not cache object greater than _ KB]: Check this item and configure the size limit of a single file to be cached. A too large file will occupy much disk space of the IAM gateway device.

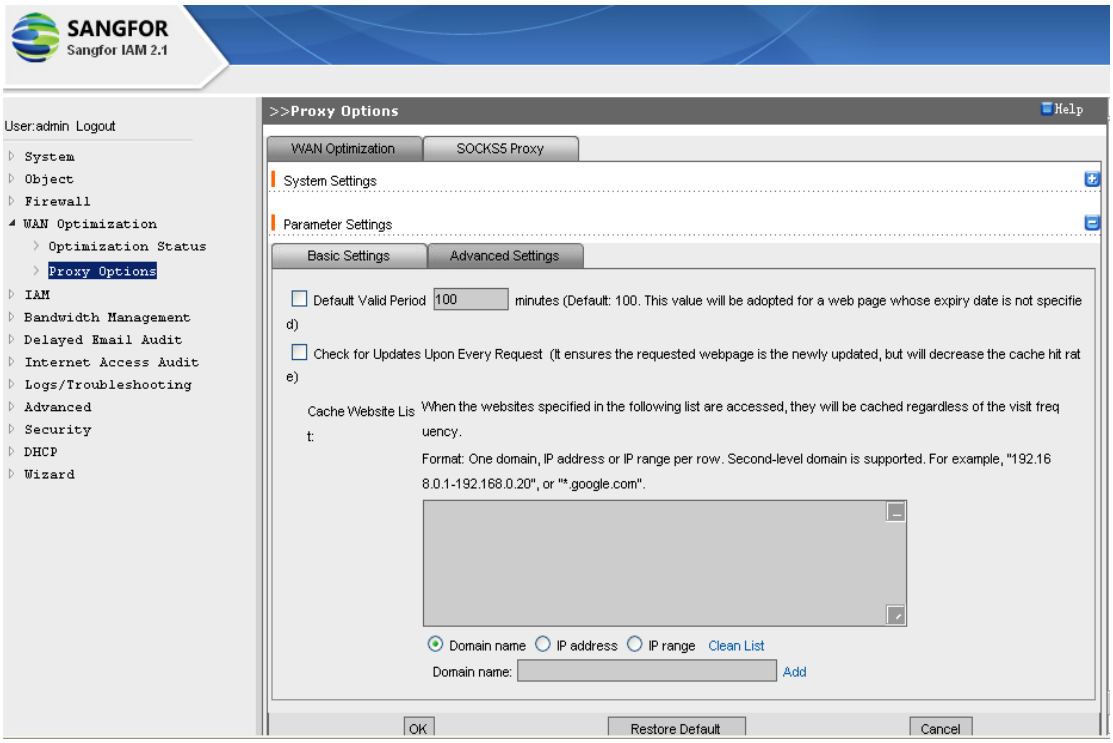
[Excluded Website List]: Configures the website(s) whose data are not to be cached. As some websites are of high instantaneity and change in real time, data of these websites need not be cached.

<Restore Default>: Click this button to restore the factory default settings.

Having completed configuring this page, you have to click the <OK> button to save the setting; or click the <Cancel> button to give up configuring this page.

6.2.1.2. Advanced Settings

[Advanced Settings]: Configures the valid time of the cached data, the method the requests are updated and the website with higher priority to be cached.



[Default Valid Period _ minutes]: Check this item and configure the update interval of the cache. Since most of the websites do not define the expiry time of a webpage, the IAM gateway device will not cache these WebPages if you leave this item unchecked (it is unchecked by default). If

this item is checked, the program will automatically define an expiry date for these WebPages.

[Check for Updates Upon Every Request]: Check this item and every request will be inspected regardless of whether the corresponding cache is the latest. For sure, the cache hit percent will lower down if it is checked.

[Cache Website List]: Configures the website(s) that has higher priority to be cached. When the websites specified in the list are visited, related data will be cached regardless of visit frequency. Enter the domain name, or IP address or IP range into the list.

<Restored Default>: Click this button to restore the factory settings.

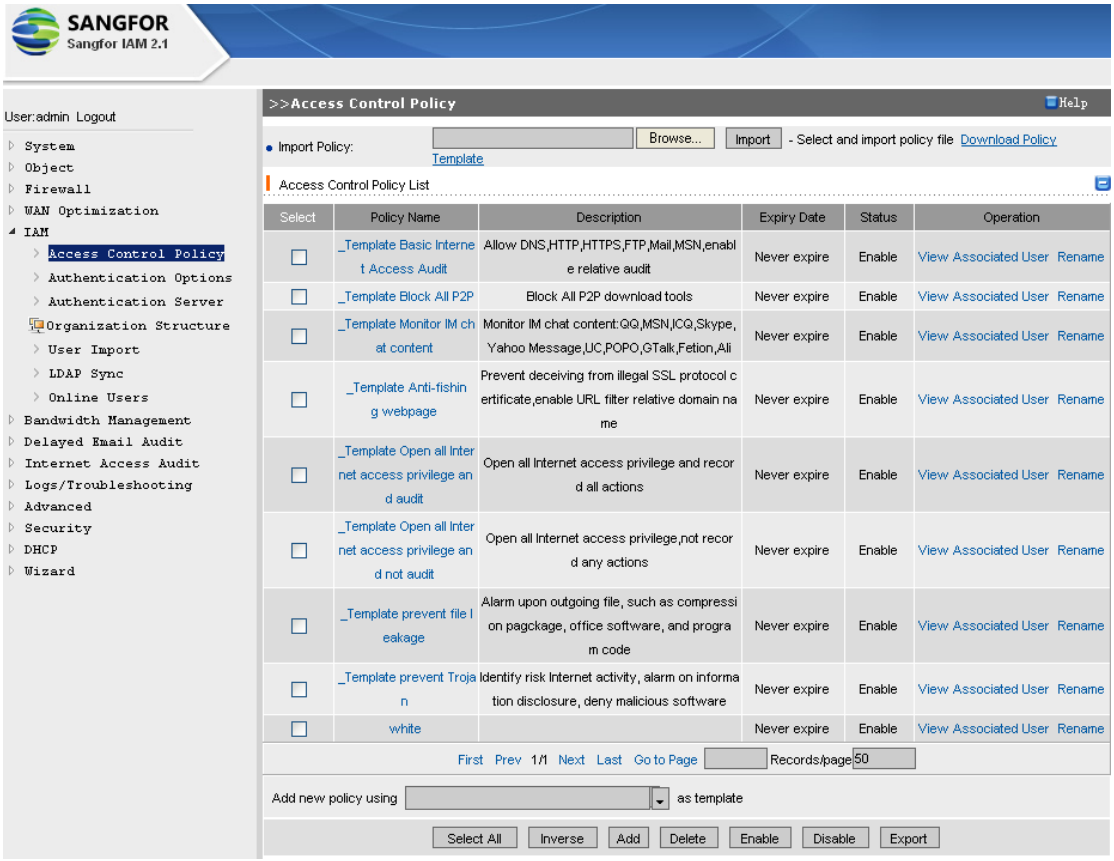
Having completed configuring the page, you have to click the <OK> button to save the settings, or click the <Cancel> button to give up configuring this page.

This section configures the global settings of the WAN optimization module. As to the configuration of disabling the WAN optimization function for a single user, please refer to Section 7.1.2.1 Access Control.

Chapter 7 IAM

[IAM] covers configuration of [Access Control Policy], [Authentication Option], [Authentication Server], [Organization Structure], [User Import], [LDAP Sync] and [Online Users].

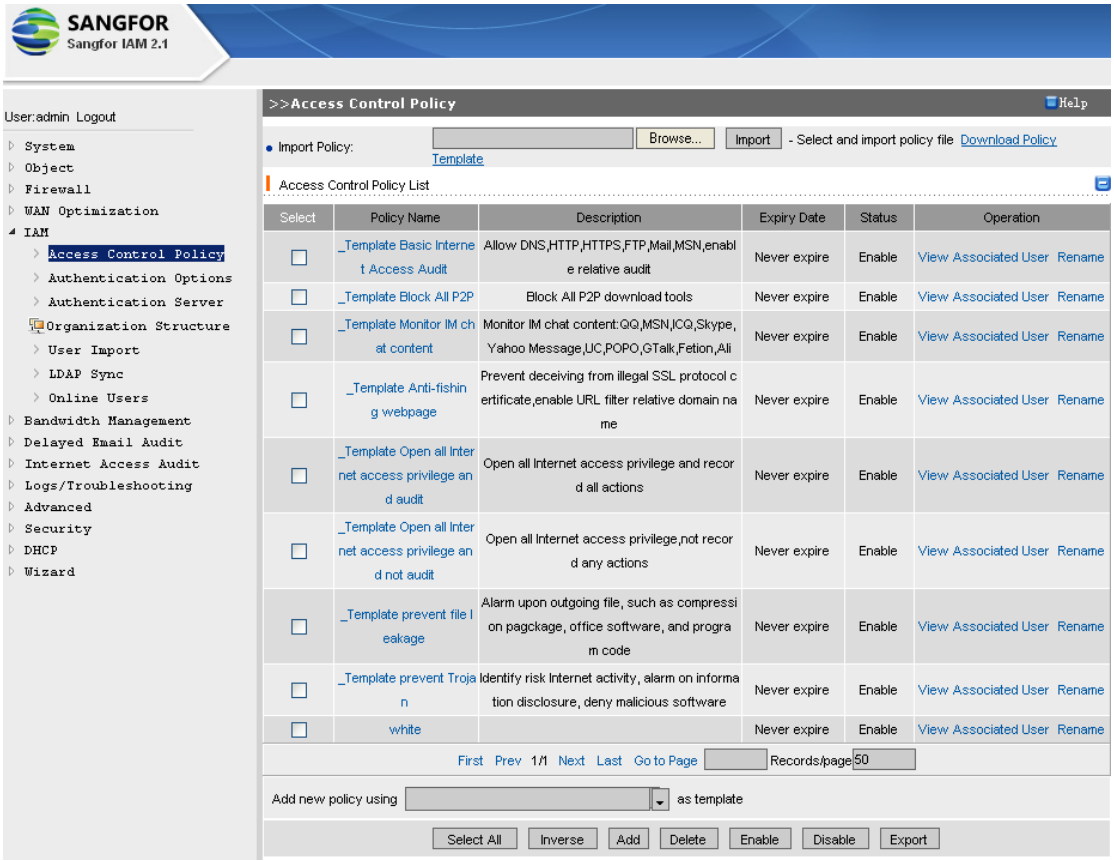
The default page is as shown below:



7.1. Access Control Policy

[Access Control Policy] mainly configures the policy controlling the LAN users to get access to the Internet. It involves the configuration of [Access Control], [Web Filter], [Email Filter], [SSL Management], [Application Audit], [Flow/Time Statistics], [Ingress System], [Risk Ident] and [Reminder]. The policies configured herein can be referenced by multiple users or user groups, so as to implement Internet access controlling and monitoring.

The default [Access Control Policy] configuration page is as shown below



[Access Control Policy List]: Displays the already-configured policies, including the information of the [Policy Name], [Description], [Expiry Date], [Status] and [Operation]

<Select All>, <Inverse>: Click this button to quickly select the needed policies.

<Add>: Click this button to create a new access control policy.

<Delete>: Click this button to delete the selected access control policy or policies.

<Enable>: Click this button to enable the selected access control policy or policies.

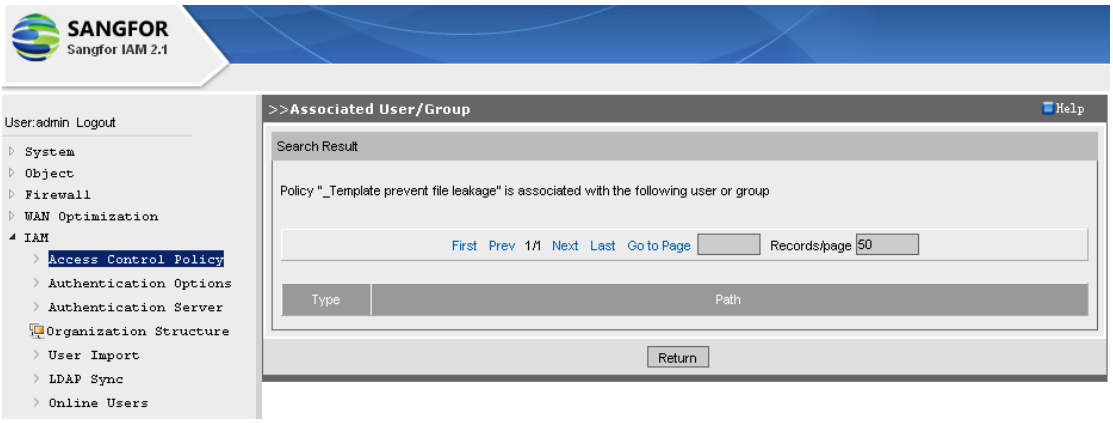
<Disable>: Click this button to disable the selected access control policy or policies.

<Export>: Click this button to export the selected access control policy or policies and save into the local computer.

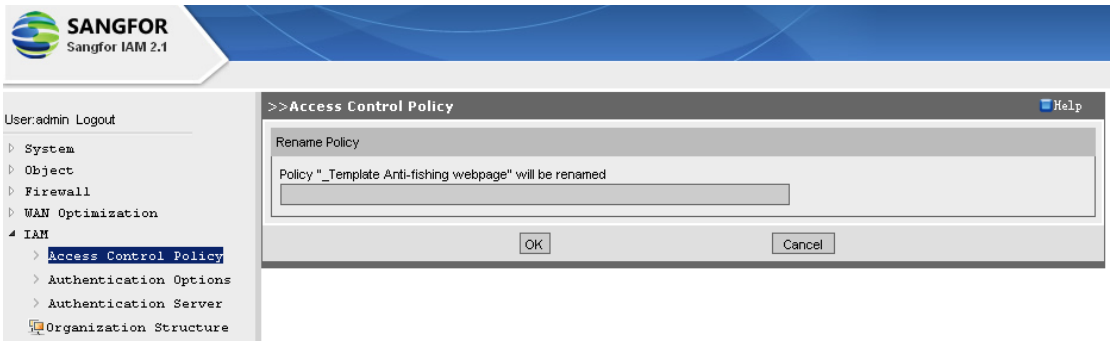
[Import Policy]: Click the <Browse> button to upload an access control policy, and then click the <Import> button to import the policy into the IAM gateway device.

<Download Policy Template>: Click this link to download the internal policy templates of the IAM gateway device.

<View Associated User>: Click this operation link in the access control policy list to view which group or user has referenced this policy, as shown below:



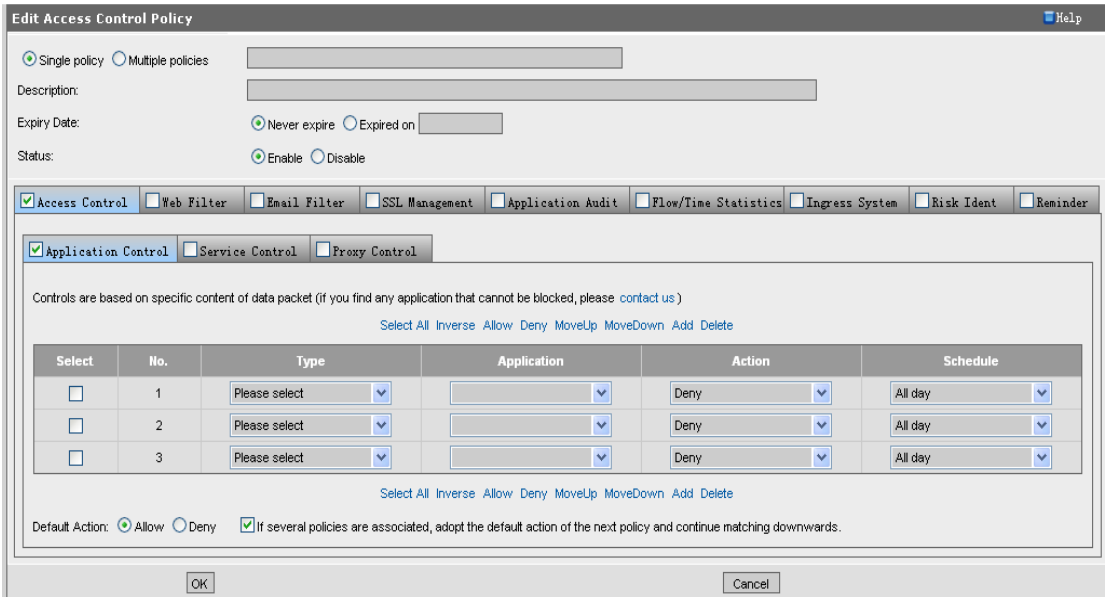
<Rename>: Click this operation link in the access control policy list to rename the policy, as shown below:



Type the new name in the text box, and then click the <OK> button to save the settings.

7.1.1. Add Access Control Policy

Under the default configuration page of [Access Control Policy], click the <Add> button to enter the [Edit Access Control Policy] page, as shown below:



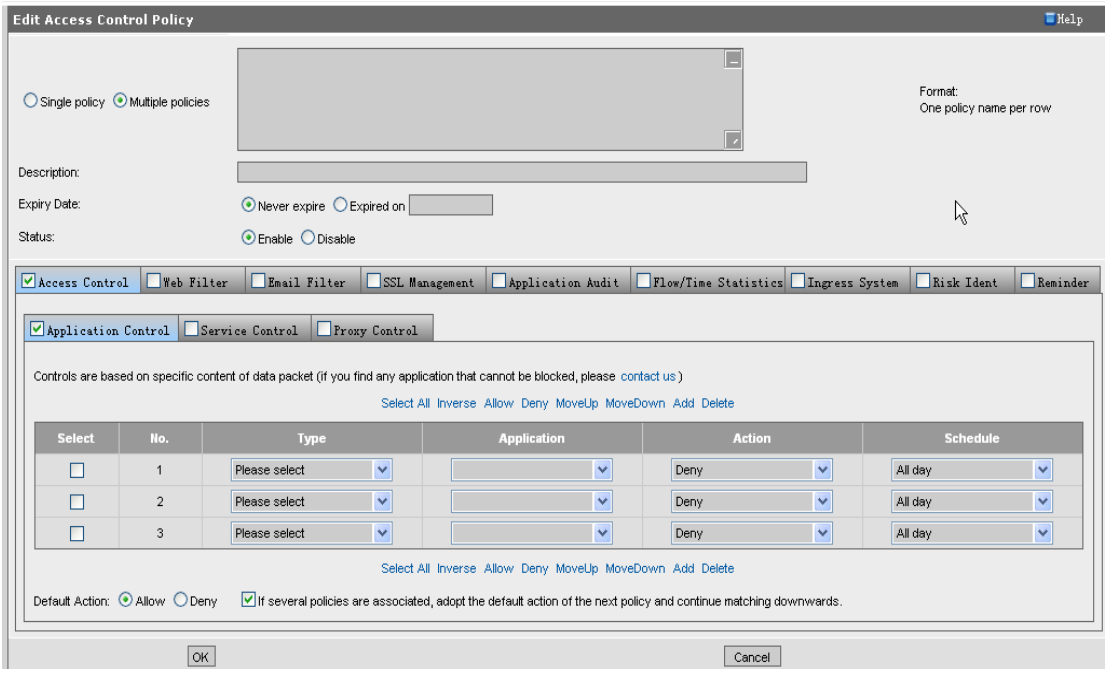
[Single policy], [Multiple policy]: Select either of the options and then type the name in the text box (better easy for memory) to distinguish it from others.

[Description]: Enter a brief description for this access control policy.

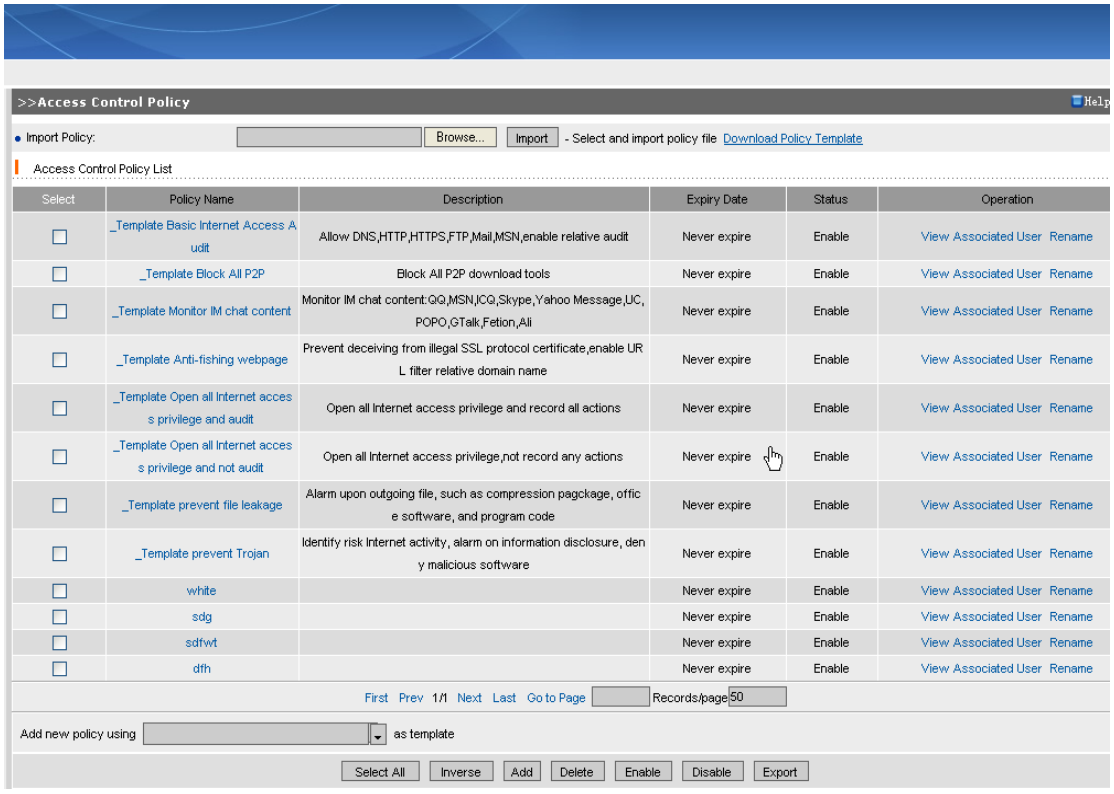
[Expiry Date]: Select [Never expire], or select [Expired on] and configure the date.

[Status]: Configures the status of this policy itself. Select [Enable] to enable this access control policy.

Select [Single Policy] or [Multiple Policies] to add one policy or add several policies respectively. [Multiple Policies] enables you to add several policies that are of same property, as shown below:

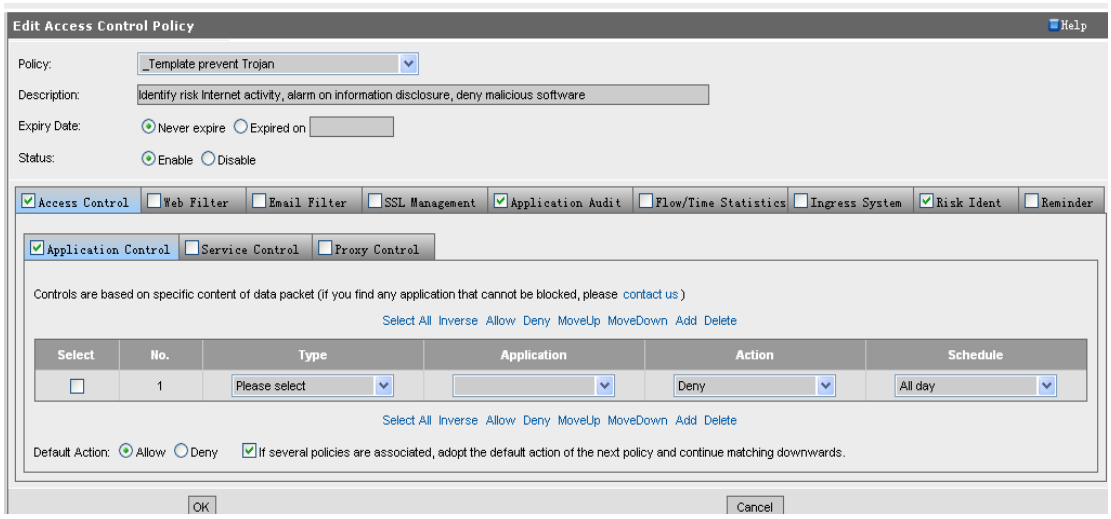


Having completed configuring the page, you have to click the <OK> button to add one policy or multiple policies, as shown below:



7.1.2. Edit Access Control Policy

Under the default configuration page of [Access Control Policy], click the name of a policy to enter the [Edit Access Control Policy] page, as shown below:



[Policy]: Select a policy to edit.

[Expiry Date]: Select [Never expire], or select [Expired on] and configure the date. The expired policy will get invalid.

[Status]: Configures the status of this policy itself, enabled or disabled. Select [Enable] to enable this access control policy.

The object of an [Access Control Policy] consists of nine modules: [Access Control], [Web Filter], [Email Filter], [SSL Management], [Application Audit], [Flow/Time Statistics], [Ingress System], [Risk Ident] and [Reminder].

The followings are detailed introductions to each module.

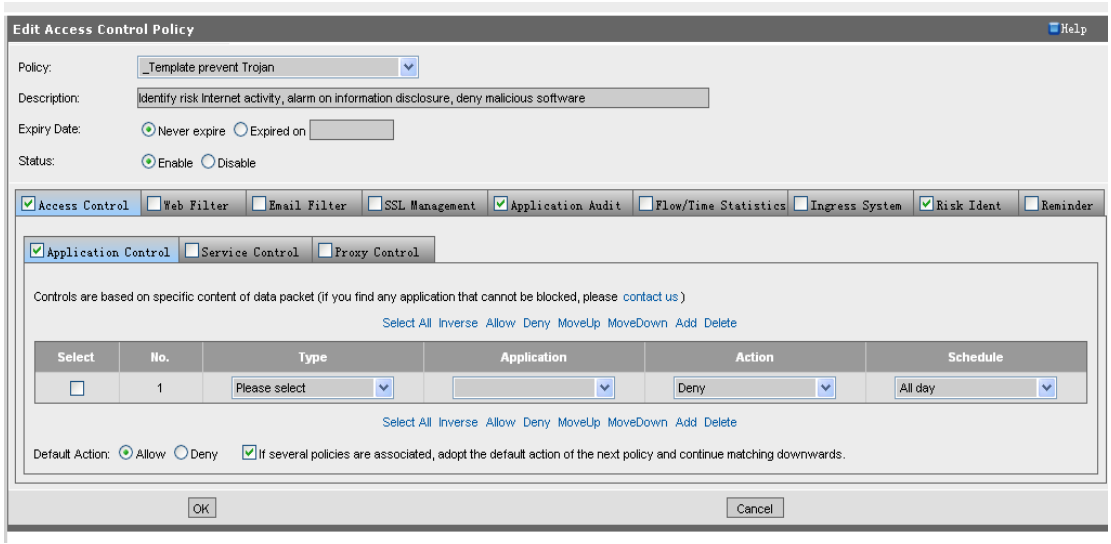
7.1.2.1. Access Control

To facilitate network administrator to control the Internet activity of the LAN users, SANGFOR IAM gateway device provides the control service based on inspecting the content of the data packets of a specific application, as well as the control function for Internet service according to the destination IP address, protocol port, and schedule.

[Access Control] includes configuration of [Application Control], [Service Control] and [Proxy Control].

[Access Control]: You have to check this item to activate the configurations under it.

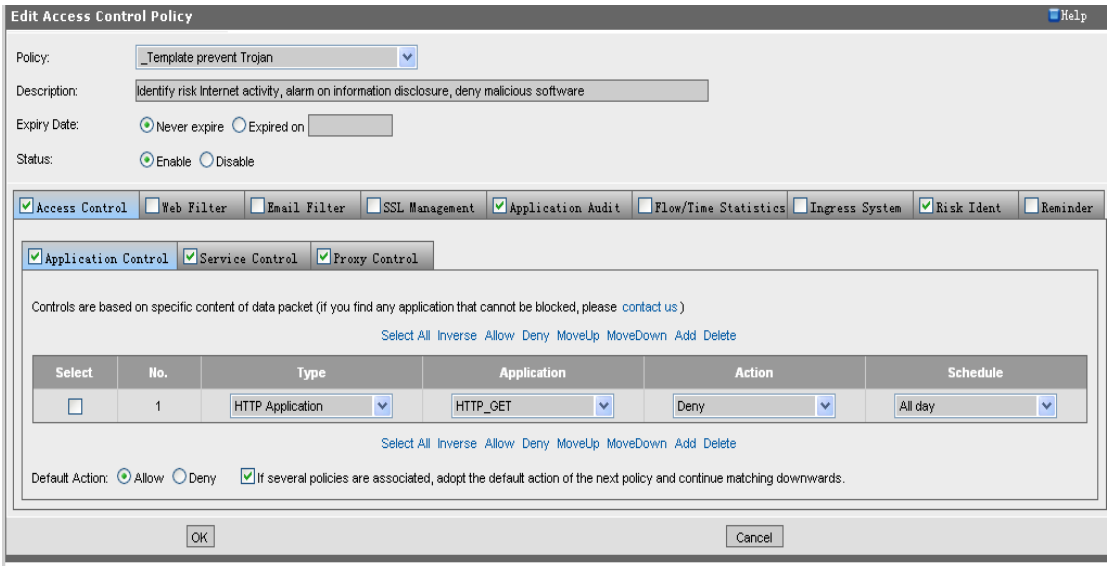
The configuration page is as shown below:



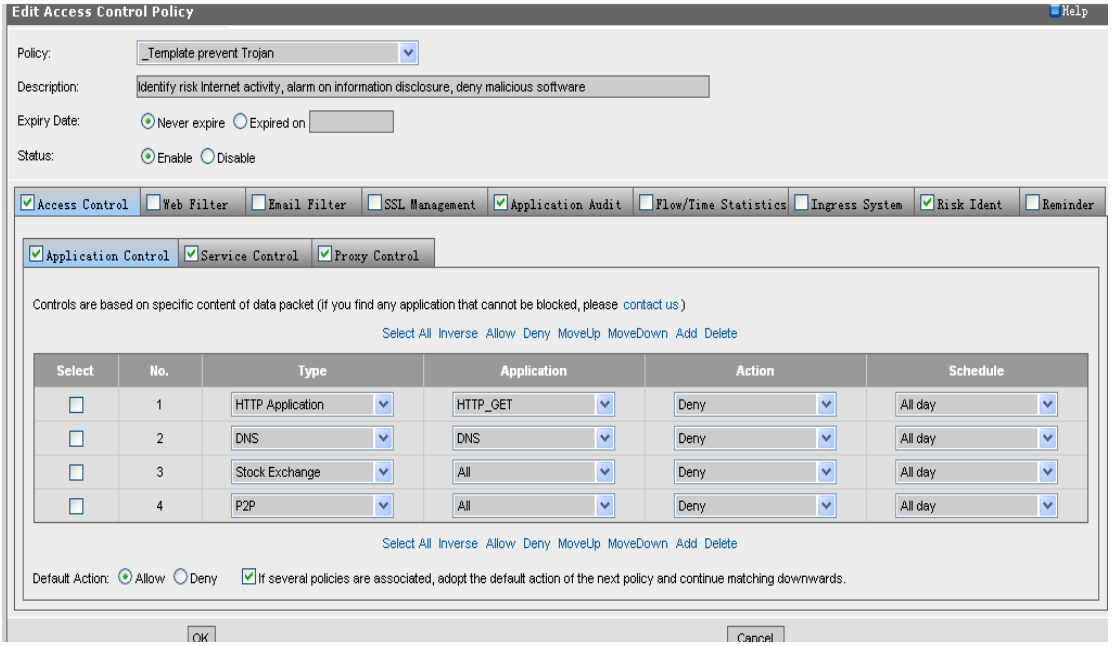
7.1.2.1.1. Application Control

[Application Control] configures the items based on which the content of data packets will be inspected, and then achieves control over certain application.

[Application Control]: You have to check it to activate the rules configured under it, as shown below:



Click the <Add> button to configure the application(s) to be controlled.



Just select application [Type], [Application], [Action] and [Schedule], and then you have finished configuring an [Application Control] rule.

For instance, if you want the LAN users to run applications only based on HTTP protocol, you need Allow ([Action]) all the HTTP applications ([Type]) and DNS application ([Type]).

<Select All>, <Inverse>: Click the button to quickly select the needed applications.

<Allow>, <Deny>, <Delete>: Click the button to allow or deny or delete the selected application(s).

<Move Up>, <Move Down>: Click the button to move up or move down the corresponding selected application(s).

[Default Action]: Select [Allow] or [Deny] to configure the default action of the current access control policy to the application(s) rules that are not in the above rule list. This item functions in association with the application(s) configured above.

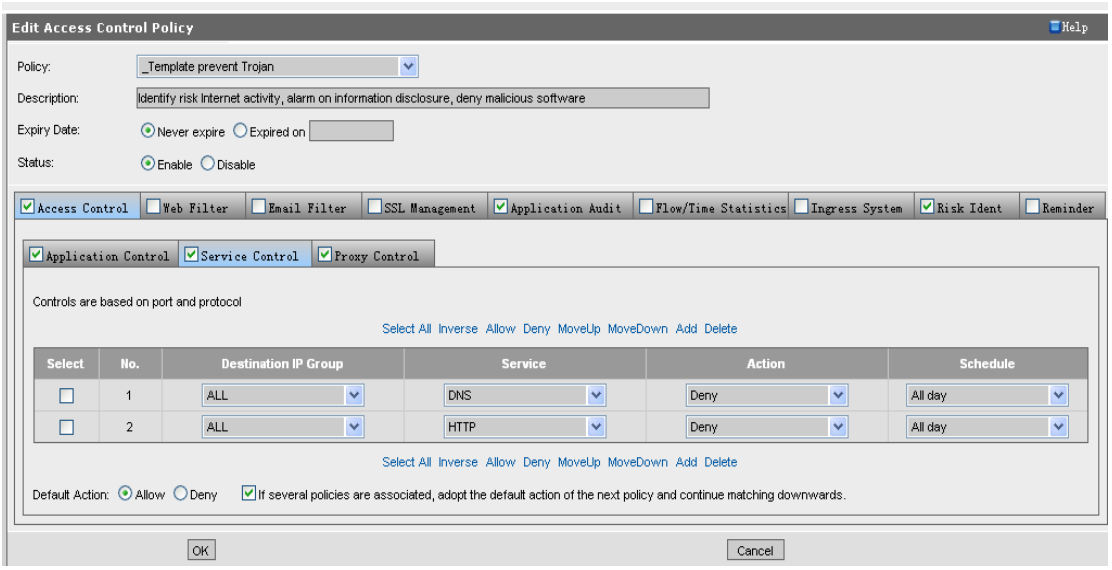
[If several policies are associated, adopt the default action of the next policy and continue matching downwards]: If multiple access control policies are associated by a user or user group, uncheck this item and the [Default Action] of the current policy will be adopted after the data packets complete matching its rules; or check this item and the data packets will continue to match the application rules of the access control policies followed.

Having completed the configuration on this page, you have to click the <OK> button to save the settings.

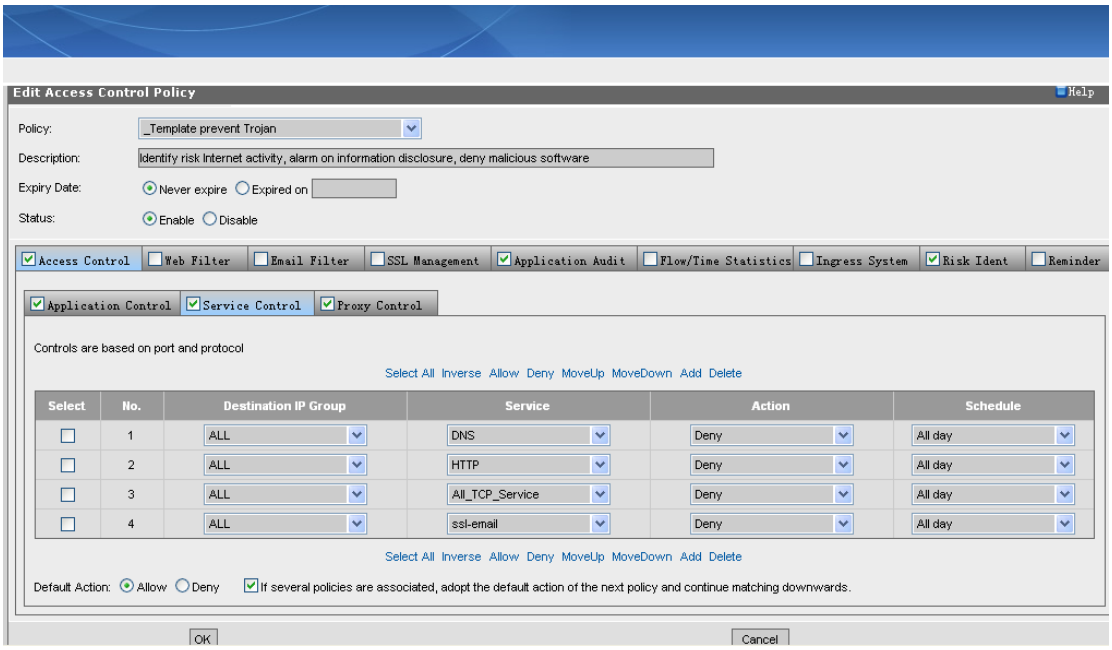
7.1.2.1.2. Service Control

[Service Control] configures the destination IP address, port and time schedule of the data packets based on which certain application will be inspected and controlled.

[Service Control]: You have to check it to activate the rules configured under it, as shown below:



Click the <Add> button to configure the service(s) to be controlled.



Just select [Destination IP], [Service], [Action] and [Schedule], and then you have finished configuring the [Service Control] rule.

For instance, if you do not want to have the LAN users to browse WebPages during office hours, you need to configure a service rule to deny HTTP service. As to the detailed introductions to configuring the [Destination IP Group], [Service] and [Schedule], please refer to the corresponding section in Chapter 4 Object.

<Select All>, <Inverse>: Click the button to quickly select the needed services.

[Allow], [Deny], [Delete]: Click the button to allow or deny or delete the selected service(s).

<Move Up>, <Move Down>: Click the button to move up or move down the corresponding selected service(s) respectively.

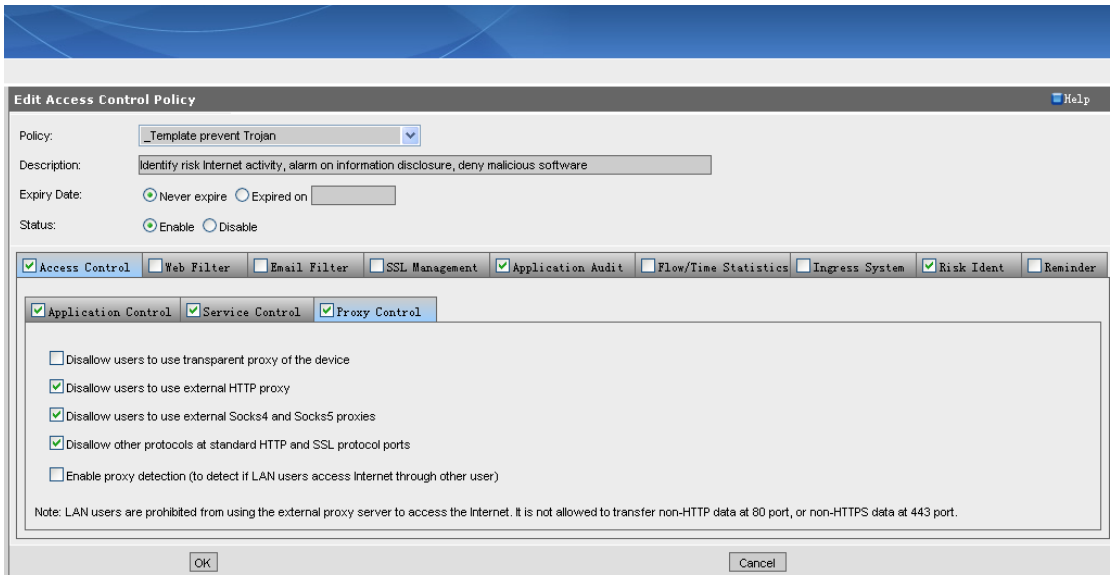
[Default Action]: Select [Allow] or [Deny] to configure the default action (of the current access control policy) for the service control rules that are not in the above rule list. This item functions in association with the service(s) configured above.

[If several policies are associated, adopt the default action of the next policy and continue matching downwards]: If multiple access control policies are associated by a user or user group, uncheck this item and the [Default Action] of the current policy will be adopted after the data packets complete matching its rules; or check this item and the data packets will continue to match the service rules of the access control policies followed.

Having completed configuring this page, you have to click the <OK> button to save the settings.

7.1.2.1.3. Proxy Control

[Proxy Control]: Check this item to activate the rules configured under it. The configuration page is as shown below:


Edit Access Control Policy
Help
Policy:
_Template prevent Trojan
Description:
Identify risk Internet activity, alarm on information disclosure, deny malicious software
Expiry Date:
Never expire
Expired on
Status:
Enable
Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
Application Control
Service Control
Proxy Control
Disallow users to use transparent proxy of the device
Disallow users to use external HTTP proxy
Disallow users to use external Socks4 and Socks5 proxies
Disallow other protocols at standard HTTP and SSL protocol ports
Enable proxy detection (to detect if LAN users access Internet through other user)
Note: LAN users are prohibited from using the external proxy server to access the Internet. It is not allowed to transfer non-HTTP data at 80 port, or non-HTTPS data at 443 port.
OK
Cancel

Check [Disallow users to use transparent proxy of the device], or [Disallow users to use external HTTP proxy], or [Disallow users to use external Socks4 and Socks5 proxies] or [Disallow other protocols at standard HTTP and SSL protocol ports].

[Disallow other protocols at standard HTTP and SSL protocol ports]: Select this item to prevent some applications from using HTTP port (TCP 80) and SSL port (TCP 443) to transmit their data, and thus disallow them to shy away from the control of the IAM gateway device.

- Some known or unknown software tools often utilize the well-known port(s) to transmit their data so as to bypass the frontend firewall, however, the contents of the data are of their own protocol format. Select [Disallow other protocols at standard HTTP and SSL protocol ports] can keep blocking the illegal data.
- Condition for selecting [Disallow users to use external HTTP proxy] or [Disallow users to use external Socks4 and Socks5 proxies] is that, the proxy is at the WAN interface end of the SANGFOR IAM gateway device. If the proxy is at the LAN interface end, then it needs to cooperate with ingress rule. As to the detailed introduction to ingress rule, please refer to Section 4. 10 Ingress Rule.

7.1.2.2. Web Filter

[Web Filter] covers the configurations of [HTTP URL Filter], [HTTPS URL Filter], [Keyword Filter], [File Type Filter], [ActiveX Filter] and [Script Filter].

[Web Filter]: Check this item to activate the rules configured under it and to enable it to filter webpage.

7.1.2.2.1. HTTP URL Filter

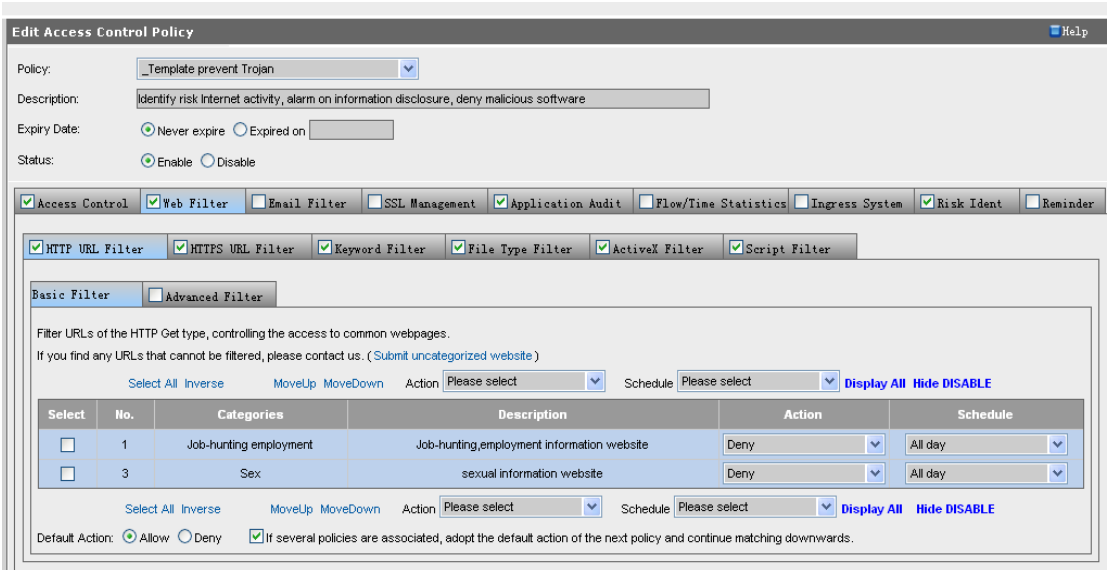
[HTTP URL Filter] includes configuration of [Basic Filter] and [Advanced Filter].

[HTTP URL Filter]: Check this item to activate the configured rules to filter HTTP URLs.

Basic Filter

[Basic Filter] functions specifically for the URL filtering of HTTP GET, mainly controlling the access to some common WebPages.

Click [Basic Filter] and the configuration page pops up as follows:



[Action]: Select [Disable], [Deny] or [Allow] define the status of the selected URL(s).

[Schedule]: Select [All day], [On duty], [Off duty] or [Internet access total time] to define the valid time of the selected URL(s). As to detailed configuration of [Schedule], please refer to Section 4.5 Schedule.

<Select All>, <Inverse>: Click this button to quickly select the needed URLs.

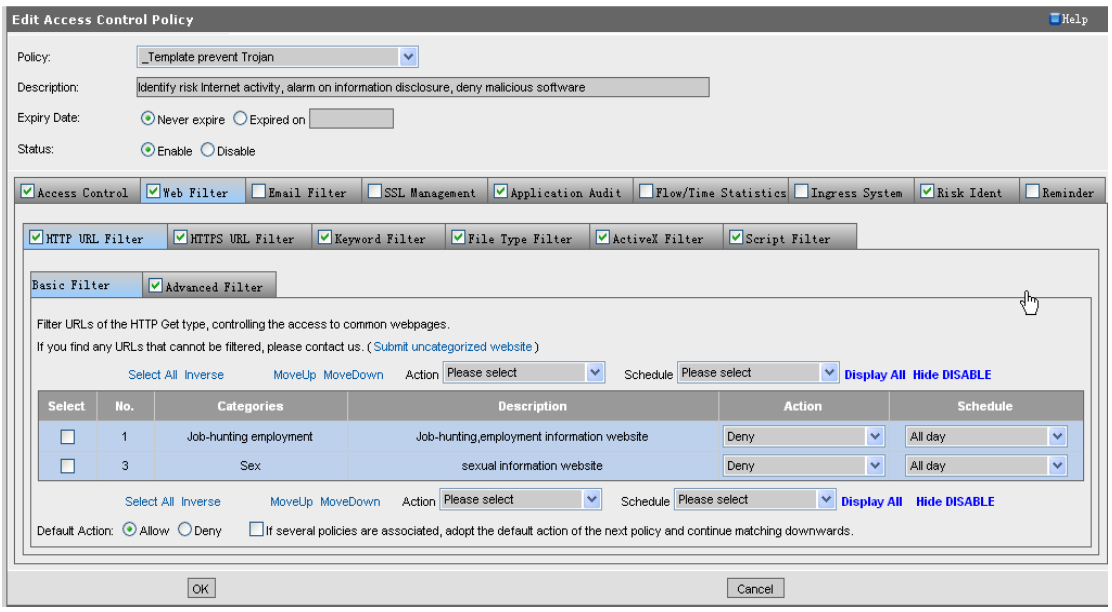
<Move Up>, <Move Down>: Click the button to move up or move down the corresponding selected URL(s).

<Display All>: Click this button to display all the URLs, including the valid URLs and the invalid URLs.

<Hide DISABLE>: Click this button to list all the valid URLs and hide all the invalid URLs.

[Default Action]: Select [Allow] or [Deny] to configure the default action of the current access control policy to the HTTP URL filter rules that are not in the above rule list. This item functions in association with the valid URL(s) configured above.

[If several policies are associated, adopt the default action of the next policy and continue matching downwards]: If multiple access control policies are associated with a user or user group, uncheck this item and the [Default Action] of the current policy will be adopted after the data packets complete matching its rules; or check this item and the data packets will continue to match the URL filtering rules of the access control policies followed.


Edit Access Control Policy
Help
Policy: _Template prevent Trojan
Description: Identify risk Internet activity, alarm on information disclosure, deny malicious software
Expiry Date: Never expire Expired on
Status: Enable Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
HTTP URL Filter
HTTPS URL Filter
Keyword Filter
File Type Filter
ActiveX Filter
Script Filter
Basic Filter
Advanced Filter
Filter URLs of the HTTP Get type, controlling the access to common webpages.
If you find any URLs that cannot be filtered, please contact us. (Submit uncategorized website)
Select All Inverse MoveUp MoveDown Action Please select Schedule Please select Display All Hide DISABLE
Select No. Categories Description Action Schedule
1 Job-hunting employment Job-hunting,employment information website Deny All day
3 Sex sexual information website Deny All day
Select All Inverse MoveUp MoveDown Action Please select Schedule Please select Display All Hide DISABLE
Default Action: Allow Deny If several policies are associated, adopt the default action of the next policy and continue matching downwards.
OK
Cancel

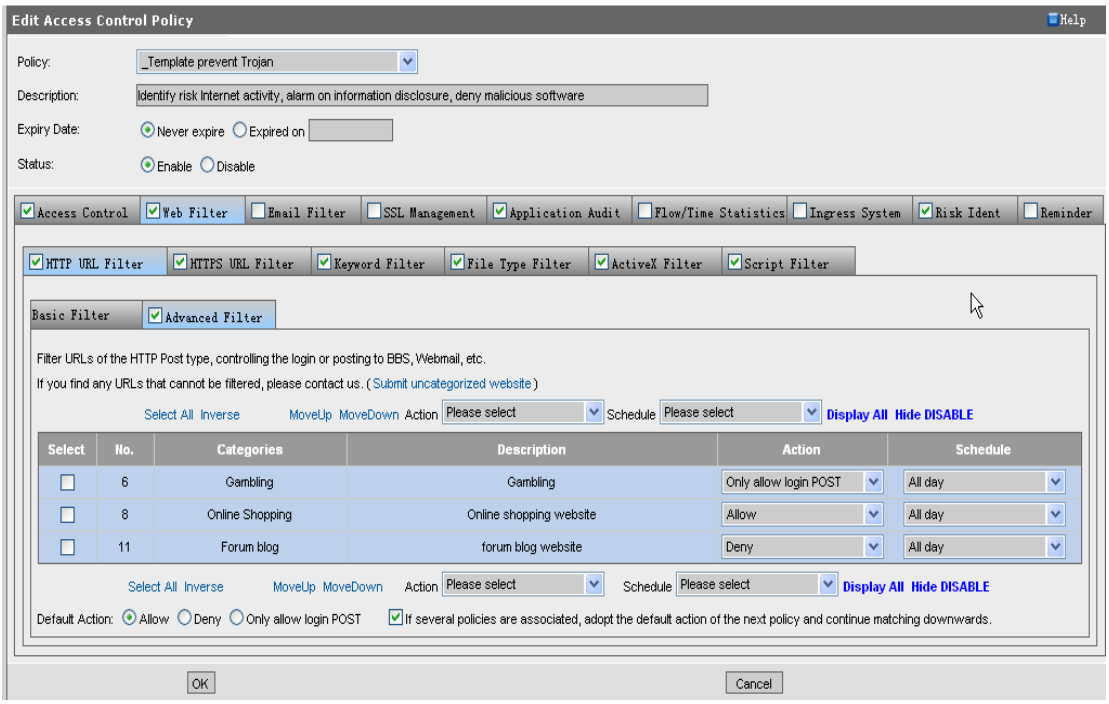
[Action]: Select [Deny] or [Allow] to define the status of the corresponding URL.

Having completed configuring this page, you have to click the <OK> button to save the settings.

Advanced Filter

[Advanced Filter] functions specifically for URL filtering of HTTP POST, controlling the process of logging in or posting to BBS, WEBMAIL, etc.

[Advanced Filter]: Check this item to activate the rules configured and enable it to do advanced filtering.


Edit Access Control Policy
Help
Policy: _Template prevent Trojan
Description: Identify risk Internet activity, alarm on information disclosure, deny malicious software
Expiry Date: Never expire Expired on
Status: Enable Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
HTTP URL Filter
HTTPS URL Filter
Keyword Filter
File Type Filter
ActiveX Filter
Script Filter
Basic Filter
Advanced Filter
Filter URLs of the HTTP Post type, controlling the login or posting to BBS, Webmail, etc.
If you find any URLs that cannot be filtered, please contact us. (Submit uncategorized website)
Select All Inverse MoveUp MoveDown Action Please select Schedule Please select Display All Hide DISABLE
Select No. Categories Description Action Schedule
6 Gambling Gambling Only allow login POST All day
8 Online Shopping Online shopping website Allow All day
11 Forum blog forum blog website Deny All day
Select All Inverse MoveUp MoveDown Action Please select Schedule Please select Display All Hide DISABLE
Default Action: Allow Deny Only allow login POST If several policies are associated, adopt the default action of the next policy and continue matching downwards.
OK
Cancel

[Action]: Select [Disable], [Deny], [Allow] or [Only allow login POST] to define the status of the selected URL(s).

[Schedule]: Select [All day], [On duty], [Off duty] or [Internet access total time] to define the valid time of the selected URL(s). As to the detailed configuration of [Schedule], please refer to Section 4.5 Schedule.

<Select All>, <Inverse>: Click this button to quickly select the needed URLs.

<Move Up>, <Move Down>: Click the button to move up or move down the corresponding selected URL(s) respectively.

<Display All>: Click this button to display all the URLs, including the valid URLs and the invalid URLs.

<Hide DISABLE>: Click this button to list all the valid URLs and hide all the invalid URLs.

[Default Action]: Select [Allow] or [Deny] to configure the default action of the current access control policy to the HTTP URL filter rules that are not in the above rule list. This item functions in association with the valid URL(s) configured above.

[Only allow login POST]: Select this item and it only allows login to WEBMAIL and BBS, view emails and read post, but does not allow email delivering and posting.

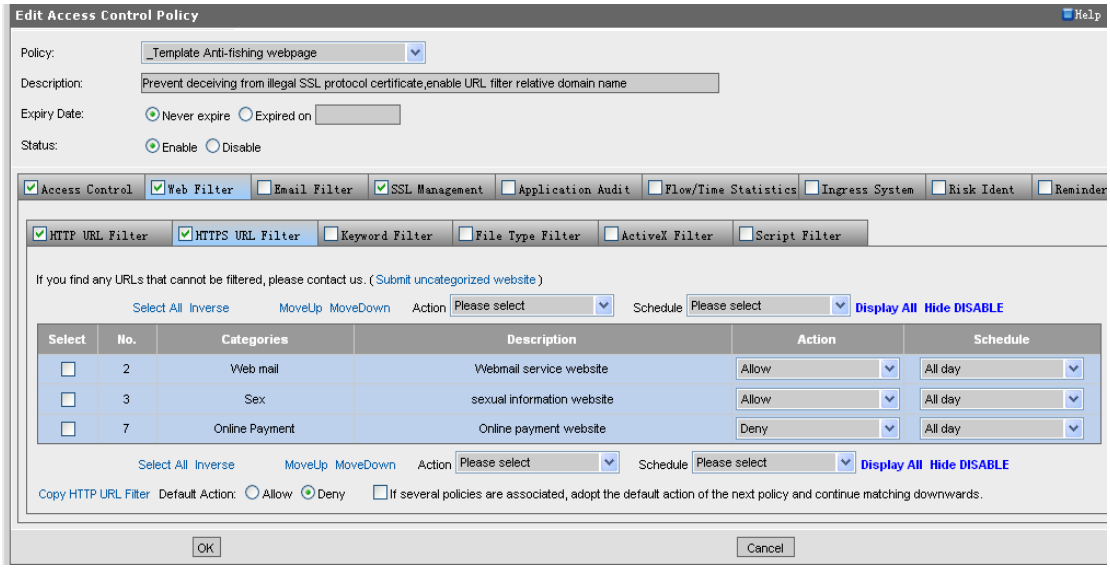
[If several policies are associated, adopt the default action of the next policy and continue matching downwards]: If multiple access control policies are associated with a user or user group, uncheck this item and the access control policy will apply the [Default Action]; or check this item and the data packets will continue to match the URL filtering rules of the access control policies followed.

Having completed configuring this page, you have to click the <OK> button to save the settings.

7.1.2.2.2. HTTPS URL Filter

[HTTPS URL Filters] configures the filtering rule for the cases that LAN users get access to website through HTTPS protocol.

[HTTPS URL Filter]: Check this item to activate the rules configured and to enable it to filter HTTPS URLs.



[Action]: Select [Disable], [Deny] or [Allow] define the status of the selected URL(s).

[Schedule]: Select [All day], [On duty], [Off duty] or [Internet access total time] to define the valid time of the selected URL(s). As to the configuration of [Schedule], please refer to Section 4.5 Schedule.

<Select All>, <Inverse>: Click this button to quickly select the needed URLs.

<Move Up>, <Move Down>: Click the button to move up or move down the corresponding selected URL(s).

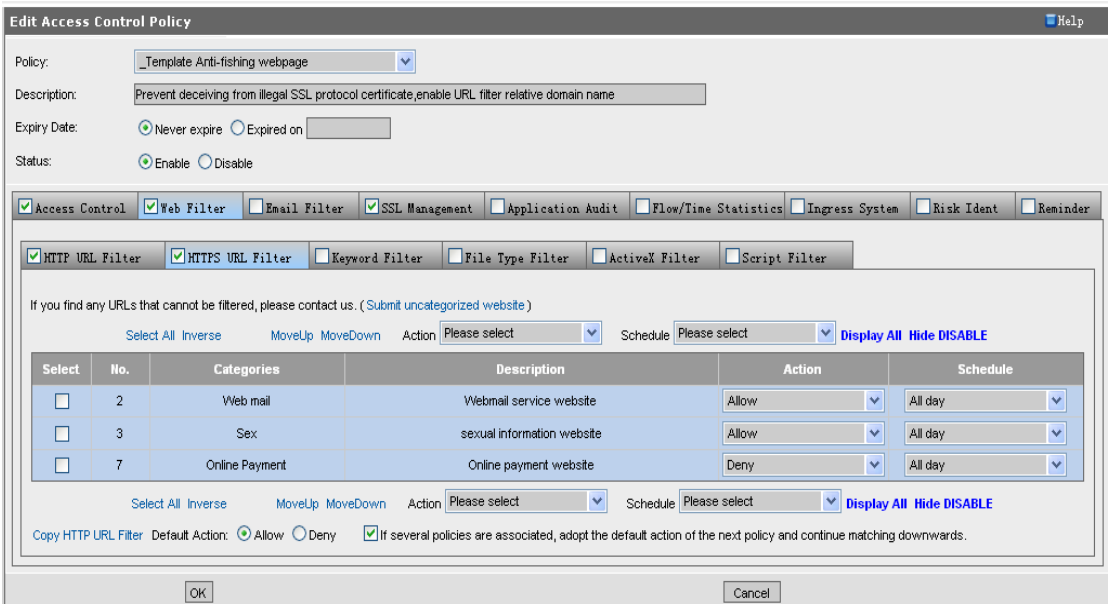
<Display All>: Click this button to display all the URLs, including the valid URLs and the invalid URLs.

<Hide DISABLE>: Click this button to list all the valid URLs and hide all the invalid URLs.

<Copy HTTP URL Filter>: Click this button, and the [HTTPS URL Filter] page will copy the configurations in [HTTP URL Filter] > [Basic Filter] page, so as to create the same rules without configuring them one by one again.

[Default Action]: Select [Allow] or [Deny] to configure the default action of the current access control policy to the HTTPS URL filter rules that are not in the above rule list. This item functions in association with the valid URL(s) configured above.

[If several policies are associated, adopt the default action of the next policy and continue matching downwards]: If multiple access control policies are associated with a user or user group, uncheck this item and the access control policy will apply the [Default Action]; or check this item and the data packets will continue to match the URL filtering rules of the access control policies followed.


Edit Access Control Policy
Help
Policy: _Template Anti-fishing webpage
Description: Prevent deceiving from illegal SSL protocol certificate,enable URL filter relative domain name
Expiry Date: Never expire Expired on
Status: Enable Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
HTTP URL Filter
HTTPS URL Filter
Keyword Filter
File Type Filter
ActiveX Filter
Script Filter
If you find any URLs that cannot be filtered, please contact us. (Submit uncategorized website)
Select All Inverse MoveUp MoveDown Action Please select Schedule Please select Display All Hide DISABLE
Select
No.
Categories
Description
Action
Schedule
2 Web mail Webmail service website Allow All day
3 Sex sexual information website Allow All day
7 Online Payment Online payment website Deny All day
Select All Inverse MoveUp MoveDown Action Please select Schedule Please select Display All Hide DISABLE
Copy HTTP URL Filter Default Action: Allow Deny
If several policies are associated, adopt the default action of the next policy and continue matching downwards.
OK
Cancel

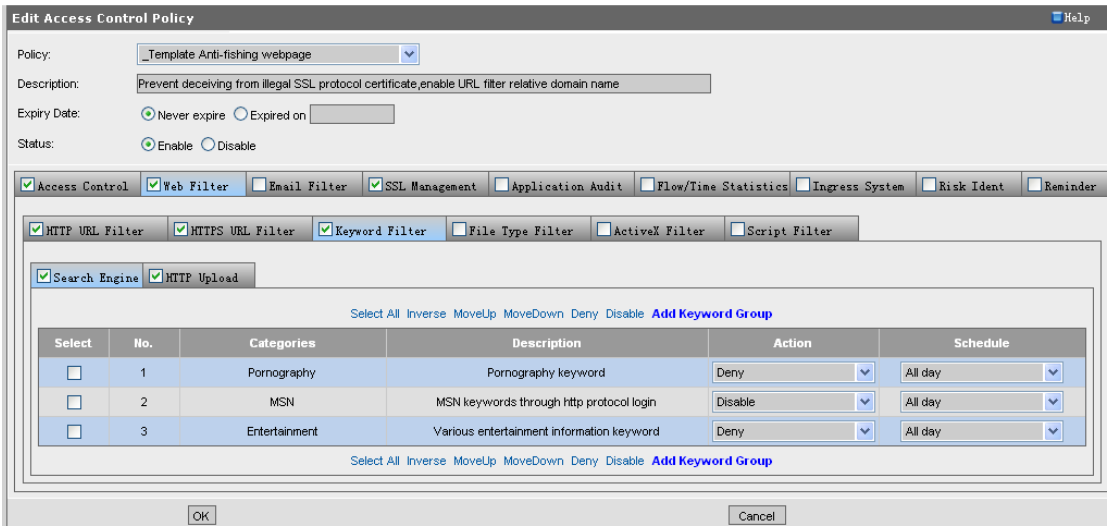
Having completed configuring this page, you have to click the <OK> button to save the settings.

7.1.2.2.3. Keyword Filter

[Keyword Filter] configures the filtering function for [Search Engine] and [HTTP Upload].

[Keyword Filter]: Check this item to activate the keyword filtering rules configured under it.

The configuration page is as shown below:



Search Engine

[Search Engine] configures some specific keywords which the LAN users may search for, and thus limit some of the behaviors of the LAN users. As to detailed procedures of configuring

keywords, please refer to Section 4.8 Keyword Group.

[Search Engine]: Check this item to enable the rules configured under it.

<Add Keyword Group>: Click this button to list the invalid keywords.

To activate the keyword(s), you have to [Select] the corresponding keyword and configure the [Action] as [Deny].

<Select All>, <Inverse>: Click the corresponding button to select the needed keyword(s).

<Move UP>, <Move Down>: Click the corresponding button to move up or move down the selected keyword(s) respectively.

<Deny>: Click this button to configure the [Action] of all the selected keyword(s) as [Deny].

<Disable>: Click this button to undo the [Deny] selection.

Having completed configuring this page, you have to click the <OK> button to save the settings.

HTTP Upload

[HTTP Upload]: Configures the filtering function for the keywords that may be uploaded through HTTP POST. For instance, if the LAN users are posting on the BBS of a forum or sending email with WEB mail server, the keyword(s) configured here will be filtered.

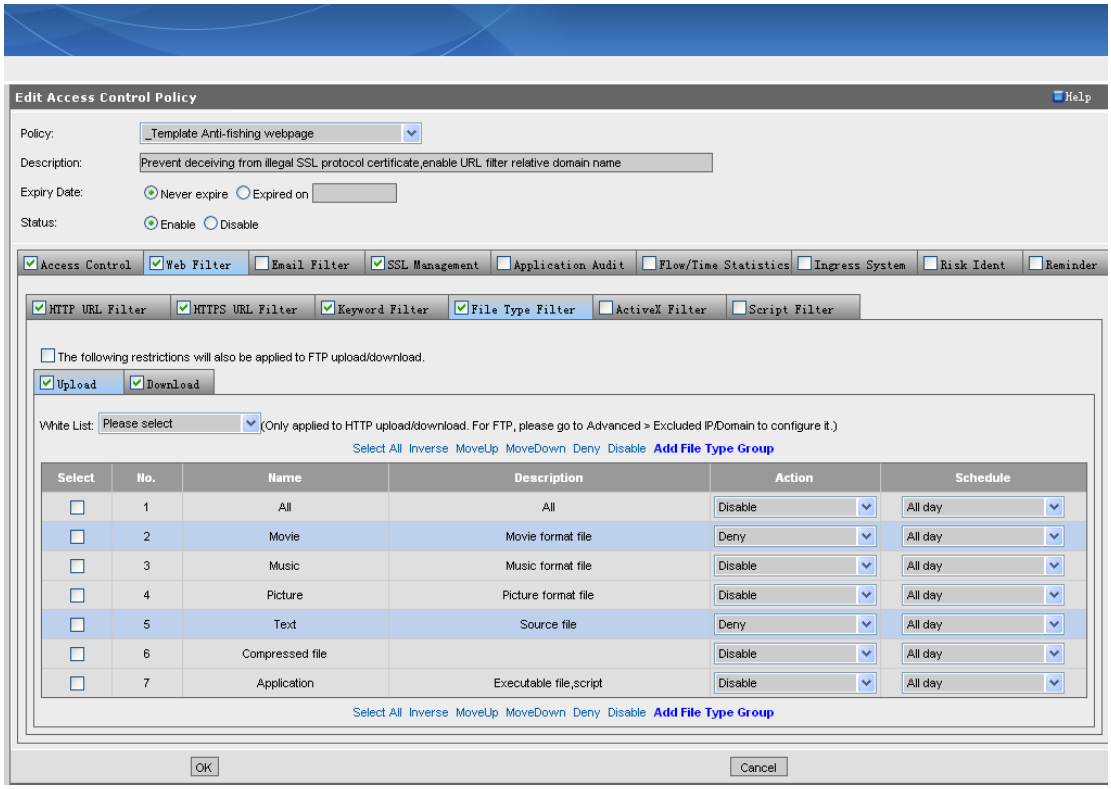
Operating procedures are the same with those of the [Search Engine]. For details, please refer to the related sections above.

[Keyword Filter] is specific for HTTP protocol.

7.1.2.2.4. File Type Filter

[File Type Filter]: Check this item to activate the file type filtering rule(s) of the access control policy.

The configuration page is as shown below:


Edit Access Control Policy
Help
Policy: _Template Anti-fishing webpage
Description: Prevent deceiving from illegal SSL protocol certificate,enable URL filter relative domain name
Expiry Date: Never expire Expired on
Status: Enable Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
HTTP URL Filter
HTTPS URL Filter
Keyword Filter
File Type Filter
ActiveX Filter
Script Filter
The following restrictions will also be applied to FTP upload/download.
Upload
Download
White List: Please select (Only applied to HTTP upload/download. For FTP, please go to Advanced > Excluded IP/Domain to configure it.)
Select All Inverse MoveUp MoveDown Deny Disable Add File Type Group
Select
No.
Name
Description
Action
Schedule
1 All All Disable All day
2 Movie Movie format file Deny All day
3 Music Music format file Disable All day
4 Picture Picture format file Disable All day
5 Text Source file Deny All day
6 Compressed file Disable All day
7 Application Executable file,script Disable All day
Select All Inverse MoveUp MoveDown Deny Disable Add File Type Group
OK
Cancel

[File Type Filter] configures filtering function for [Upload] and [Download].

[The following restrictions will also be applied to FTP upload/download]: Check this item and the filtering rules configured below will also apply to FTP upload/download.

Upload

[Upload] configures the file type filtering function to control the upload of some types of file (based on the extension name of the file). For example, if the LAN users are uploading attachment(s) through WebMail or through BBS, the access control policy will filter the limited file type(s).

[Upload]: Check this item to enable the function of filtering the to-be-uploaded file types. Except checking the [Upload] item, to achieve this filtering function, you have to add the keyword(s) to the [File Type Group] list (configured in [Object] > [File Type Group] page, please refer to Section 4.9 File Type Group).

[White List Group]: You can configure the white list group here, which is only valid for HTTP upload/download. For detailed configuring procedures, please refer to Section 4.7 White List Group.

<Add File Type Group>: Click this button to configure/activate the file type groups which have been configured in [Object] > [File Type Group] page.

To activate the file type(s), select the corresponding keyword(s) and configure the [Action] as [Deny].

<Select All>, <Inverse>: Click the corresponding button to select the needed file type(s).

<Move UP>, <Move Down>: Click the corresponding button to move up or move down the selected file type(s).

<Deny>: Click this button to configure the [Action] of the selected file type(s) as [Deny].

<Disable>: Click this button to undo the [Deny] selection.

Having completed configuring this page, you have to click the <OK> button to save the settings.

Download

[Download] configures the file type filtering function to control the download of some types of file (based on the extension name of the file). For example, if the LAN user is downloading MP3 or movie file, the access control policy will filter these files. Operating procedures are similar to those of [Upload]; for details, please refer to the related sections above.

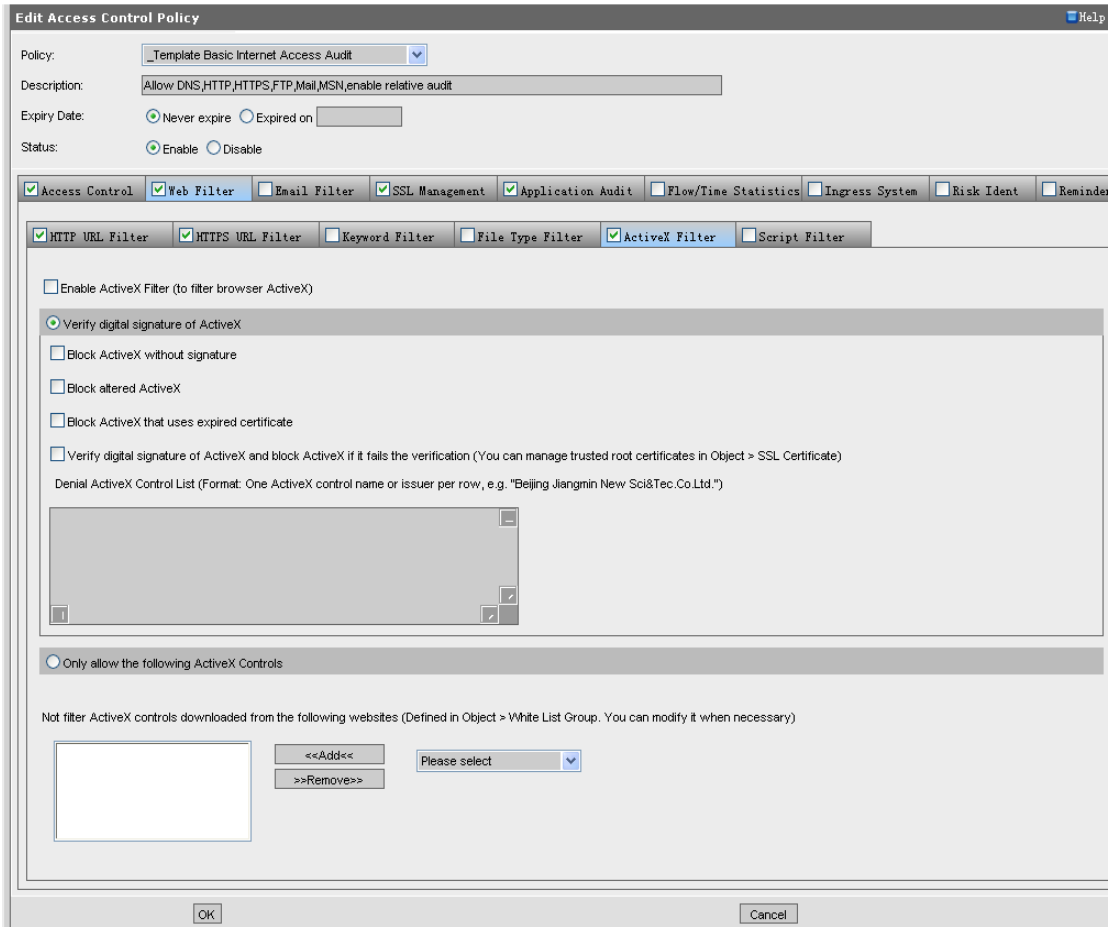
- The rules configured under the [Upload] and [Download] page are specific for HTTP (or FTP), therefore, the IAM gateway device will only inspect and analyze the extension names of the files that are transmitted through the WEB and FTP communication ports.
- [White List Group] is only valid for HTTP upload/download.
- You can add maximum 16 white list groups; each white list group supports maximum 512 URL entries.
- The domain name in the white list group can be incompletely matched. For instance, as to the domain name "*baidu.com*", it indicates *www.baidu.com*, *tieba.baidu.com*, *music.Baidu.com*, etc.
- There is a file type filter [All] which indicates all the file types. Please do select it with caution, for it will affect Internet access if the [Action] of this rule is [Deny].

7.1.2.2.5. ActiveX Filter

It happens that the installed ActiveX controls of some WebPages will affect the function of your browser, or even monitor your behavior surfing on the Internet and disclose your personal information. Some of these ActiveX controls often are installed automatically by the browser, leading to spread of malicious plug-ins. SANGFOR gateway device can effectively solve this problem, with the help of [ActiveX Filter] rule.

Any ActiveX control will be required with signature, and the untrusted plug-in will be unable to be installed into the LAN computers. In this way, security of the local area network would be guaranteed.

[Enable ActiveX Filter]: Check this item to activate the ActiveX control filtering function, and then the configurations on [Verify digital signature of ActiveX] and [Only allow the following ActiveX Controls] pages will take effect.


Edit Access Control Policy
Help
Policy:
_Template Basic Internet Access Audit
Description:
Allow DNS,HTTP,HTTPS,FTP,Mail,MSN,enable relative audit
Expiry Date:
Never expire
Expired on
Status:
Enable
Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
HTTP URL Filter
HTTPS URL Filter
Keyword Filter
File Type Filter
ActiveX Filter
Script Filter
Enable ActiveX Filter (to filter browser ActiveX)
Verify digital signature of ActiveX
Block ActiveX without signature
Block altered ActiveX
Block ActiveX that uses expired certificate
Verify digital signature of ActiveX and block ActiveX if it fails the verification (You can manage trusted root certificates in Object > SSL Certificate)
Denial ActiveX Control List (Format: One ActiveX control name or issuer per row, e.g. "Beijing Jiangmin New Sci&Tec.Co.Ltd.")
Only allow the following ActiveX Controls
Not filter ActiveX controls downloaded from the following websites (Defined in Object > White List Group. You can modify it when necessary)
<<Add<<
>>Remove>>
Please select
OK
Cancel

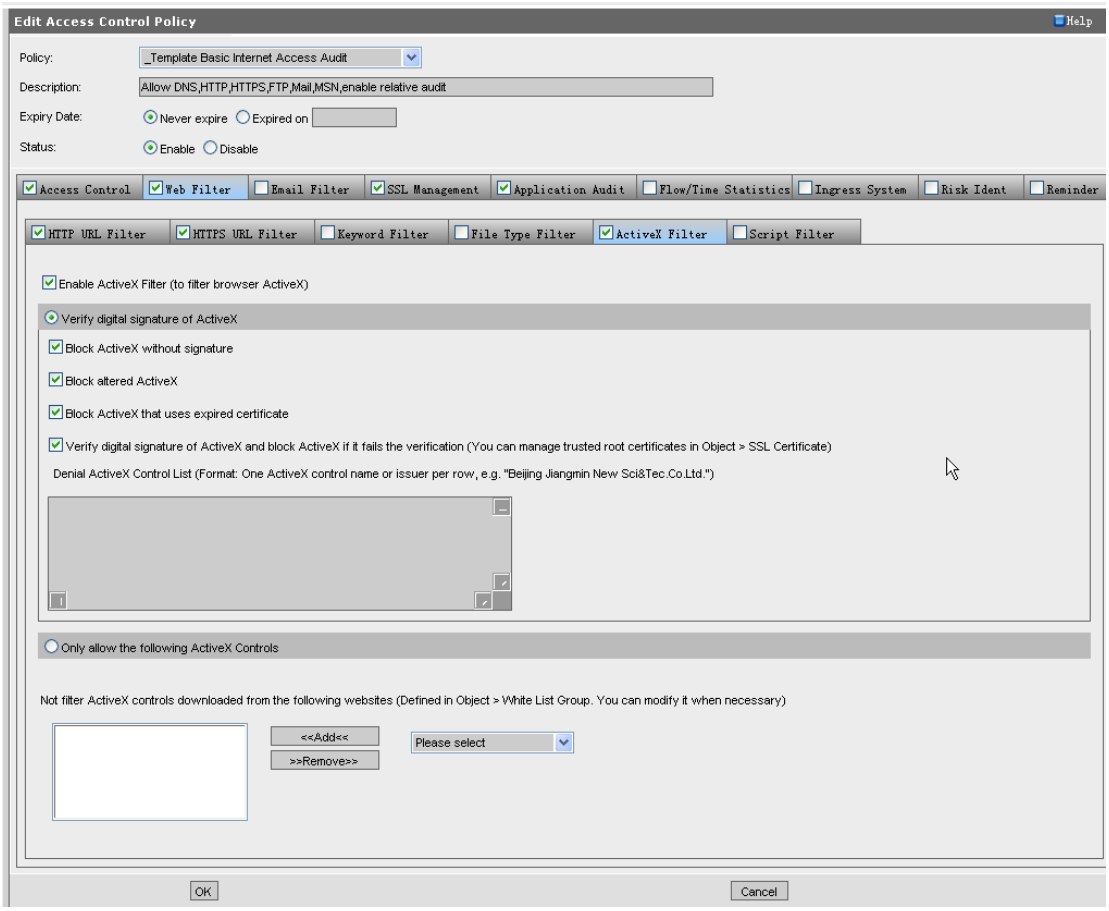
[ActiveX Filter] includes [Verify digital signature of ActiveX] and [Only allow the following ActiveX Controls], and [Not filter ActiveX controls downloaded from the following websites]; as

to the former two, only one of them can be selected.

Verify Legality of the Signature

[Verify digital signature of ActiveX]: Select this item, and you can configure the conditions to verify the legality of the certificate (signature).

The configuration page is as shown below:



[Block ActiveX without signature]: Check this item, and the access control policy will require signature from the ActiveX control. If the ActiveX control has no signature, it will be filtered.

[Block altered ActiveX]: Check this item, and the access control policy will inspect whether the signature of the ActiveX control is altered. If the signature of the ActiveX control has been altered, it would be filtered.

[Block ActiveX that uses expired certificate]: Check this item, and the access control policy will inspect whether the signature of the ActiveX control is expired. If the signature of the ActiveX control has expired, it would be filtered.

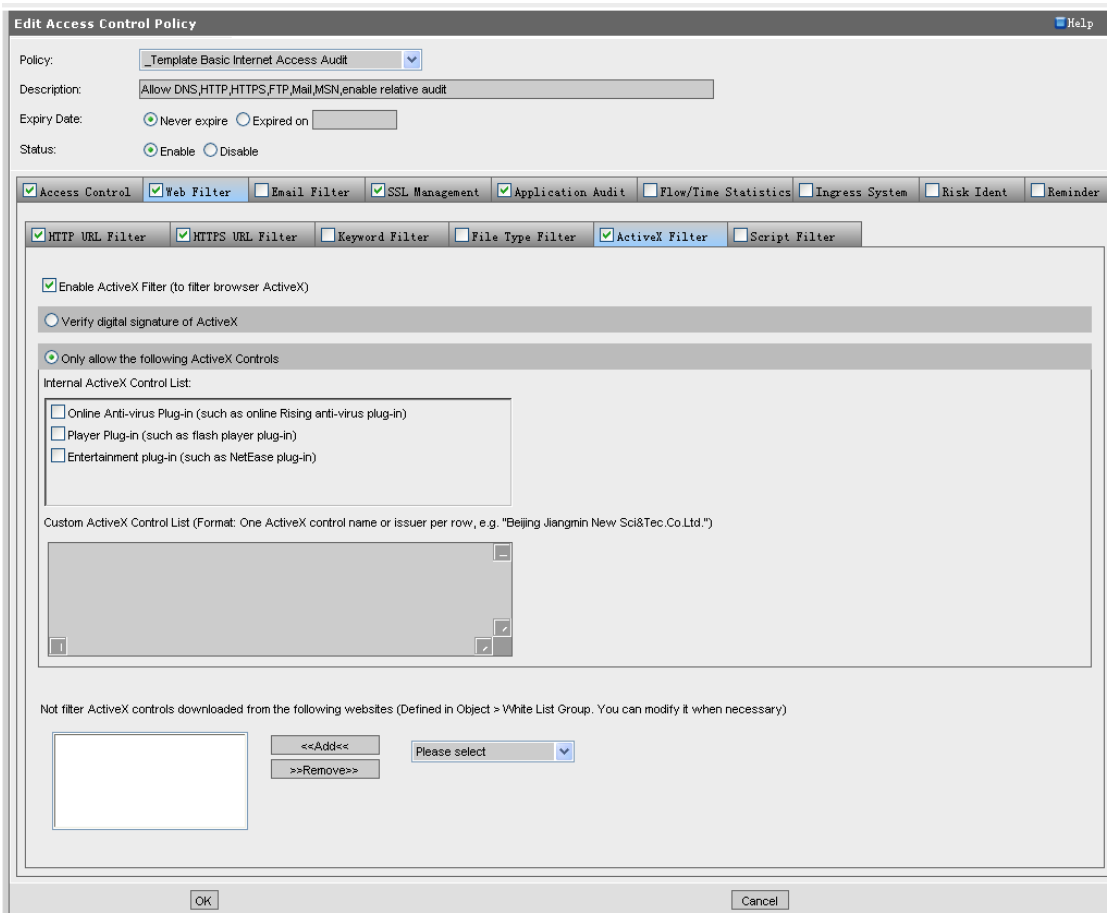
[Verify digital signature of ActiveX and block ActiveX control if it fails the verification]: Check

this item, and the access control policy will check whether the certificate (signature) of the ActiveX control exists in the [Trusted Root Certificate List]. If certificate does not exist in the list, the ActiveX control will be filtered. As to the management of certificates, please refer to Section 4.11 SSL Certificate.

[Denial ActiveX Control List]: Configures the keywords may contained in the ActiveX control, one ActiveX control or issuer per row. If the keyword is detected in the plug-in, it will be filtered. It should be noted that the keyword configured here does not support wildcard characters, length of each keyword within 64 bytes, and total keywords within 32.

Only Allow the Following ActiveX Controls

[Only allow the following ActiveX Controls]: Check this item, and you can configure the conditions for installing ActiveX controls. The to-be-installed ActiveX control will be marked as secure if it matches any of that in the [Internal ActiveX Controls List]. In this way, the LAN users can be protected from potential malicious plug-ins from external networks.



[Internal ActiveX Control List] configures three types of plug-in, namely, [Online Anti-virus Plug-in], [Player Plug-in] and [Entertainment plug-in].

[Online Anti-virus Plug-in]: Check this item, and the plug-in will be allowed to install if it is a kind of online anti-virus plug-in.

[Player Plug-in]: Check this item, and the plug-in will be allowed to install if it is a kind of player plug-in.

[Entertainment Plug-in]: Check this item, and the plug-in will be installed if it is a kind of entertainment plug-in.

[Custom ActiveX Control List]: Configures the keywords may contained in the to-be-installed ActiveX control, one ActiveX control or issuer per row. If the keyword is detected in the plug-in, it will be defined as secure and be installed. It should be noted that the keyword configured here does not support wildcard characters, length of each keyword within 64 bytes, and total keywords within 32.

Not Filter ActiveX Controls Downloaded From the Following Websites

[Not filter ActiveX controls downloaded from the following websites]: You can add the websites (among those in the white list group) which will not be filtered. The access control policy will not filter the plug-ins of the websites in this list. As to the configuration of white list group, please refer to Section 4.7 White List Group.

Click the pull-down menu and select a needed white list; then click the <Add> button to add the white list to the box. To remove a white list from the box, just select the white list and click the <Remove> button.

Having configured all the filtering conditions, you have to click the <OK> button to save all the settings.

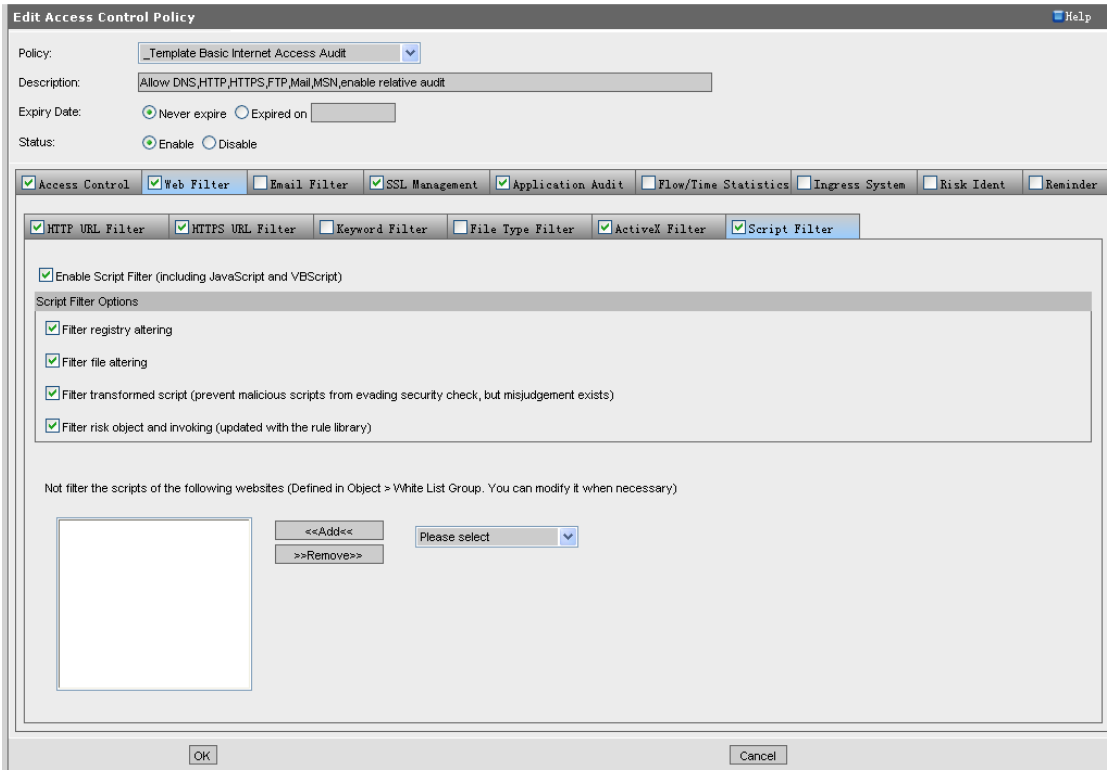
- [ActiveX Filter] is only applicable to the ActiveX controls.
- Some ActiveX controls are not downloaded from the current visited page but from the link of another website. To get known the source of the plug-in, LAN user can enter the data center and view the Website Access (website browse) statistics. If this plug-in is filtered, detailed information of this plug-in will be recorded in Data Center.

7.1.2.2.6. Script Filter

Internet security increasingly becomes a severe problem, visiting a bad website will infect the device with Trojan or other kinds of viruses which are caused by running risky scripts.

SANGFOR IAM gateway device can identify the features of the scripts of the browsed webpage, and block these scripts before they are downloaded to the browser; therefore, the LAN users are kept away from the script viruses.

[Script Filter]: Check this item to activate the script filtering function and the built-in (internal) rules will take effect (functioning for controlling the illegal scripts). SANGFOR IAM gateway device can filter JavaScript and VBScript.



[Script Filter Options] includes configurations of [Filter registry altering], [Filter file altering], [Filter transformed script] and [Filter risk object and invoking].

[Filter registry altering]: Check this item, and the script will be filtered directly if it has ever altered the registry.

[Filter file altering]: Check this item, and the script will be filtered directly if it has ever altered the file.

[Filter transformed script]: Check this item to disallow the script to shy away from inspection. This operation may cause misjudgment.

[Filter risk object and invoking]: Check this item, and the script will be directly filtered if it contains risky object and invoking.

[Not filter the script of the following websites]: You can add the websites (among those in the white list group) whose scripts will not be filtered. Click the pull-down menu and select a needed white list; then click the <Add> button to add the white list to the box. To remove a white list from the box, just select the white list and click the <Remove> button. As to the configuration of white list group, please refer to Section 4.7 White List Group.

Having completed configuring this page, you have to click the <OK> button to save the settings.

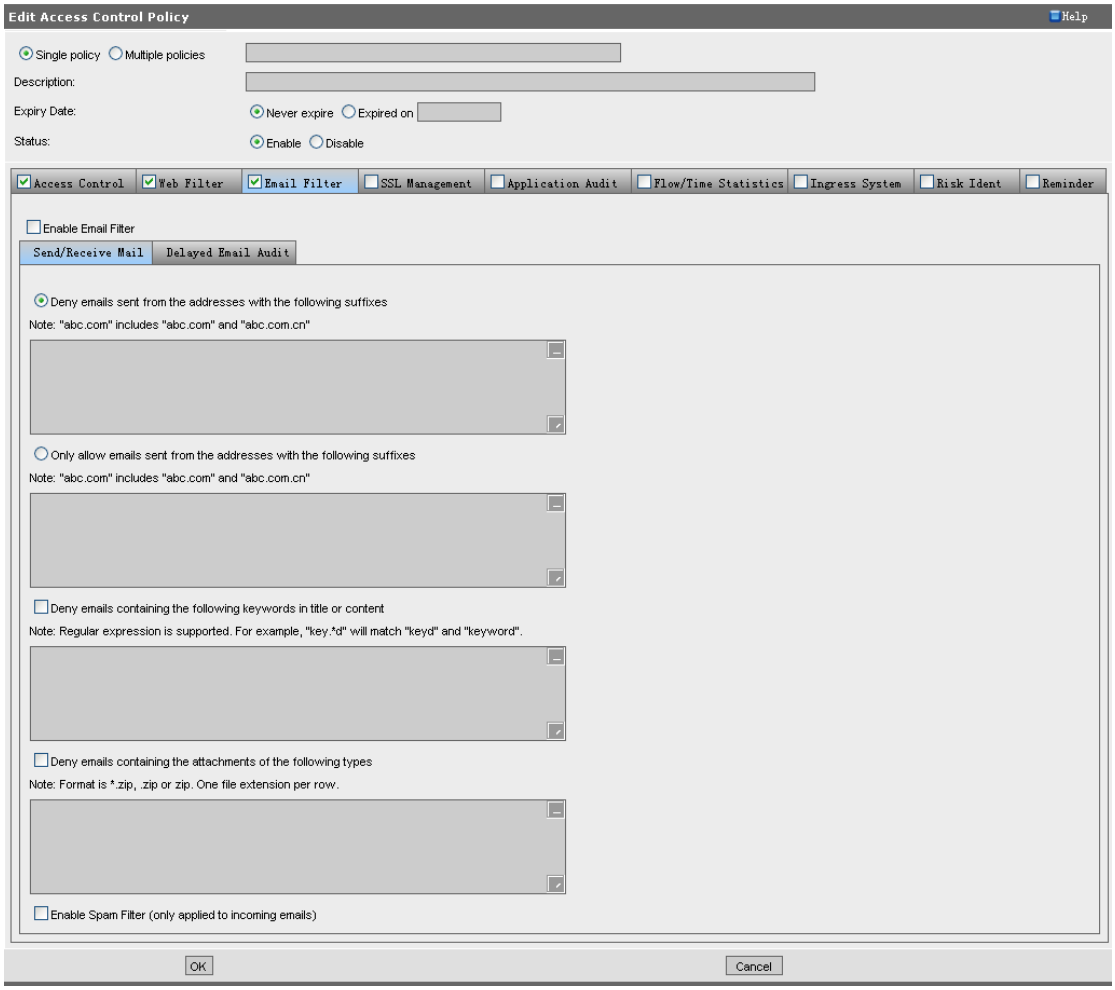
7.1.2.3. Email Filter

7.1.2.3.1. Send/Receive Mail

[Email Filter] mainly is used for limiting, monitoring, filtering the sent or received emails, or delaying sending or receiving these emails for audit, etc., while the LAN users are using the email client to send or receive email with POP3/SMTP protocol. [Email Filter] covers configurations of [Send/Receive Mail] and [Delayed Email Audit].

[Send/Receive Mail] is mainly used for controlling and delaying the delivery of the emails, and sending the delayed emails for audit, in association with the configurations of source address, email title, email contents and attachment file type. For detailed configuration guide, please follow the notes on the interface.

The configuration page is as shown below:



[Email Filter], [Enable Email Filter]: Check the two items to activate the email filtering function.

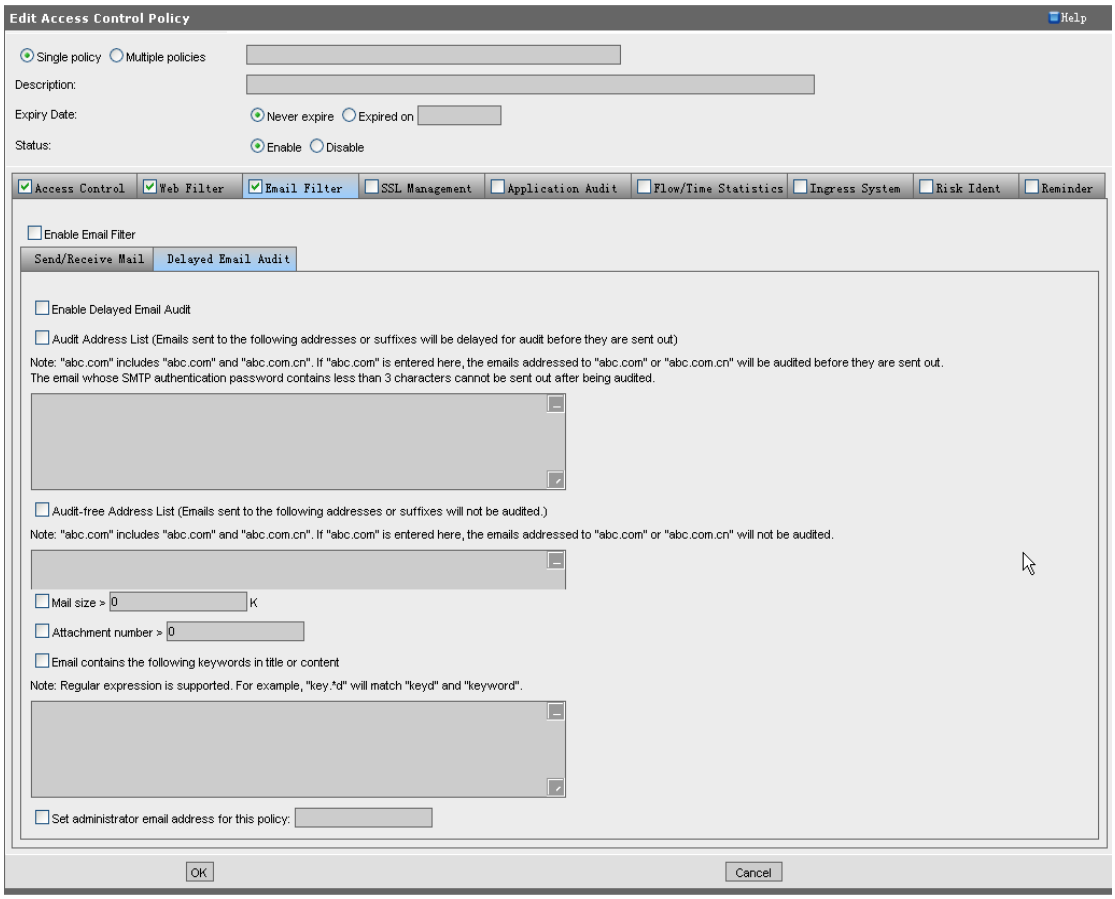
For instance, if you want the LAN users use only the email address provided by the enterprise itself, select [Only allow emails sent from the addresses with the following suffixes], and then type the *vpn.com.cn* in the text box. This configuration will allow the LAN users to send or receive emails only through the email addresses with the *@vpn.com.cn* suffix.

[Deny emails containing the following keywords in title or content] and [Deny emails containing the attachments of the following types] are applied to sending emails by the LAN users. Check the corresponding item and type the keyword or extension name of the attachment in the text box, one entry (keyword or extension name) per row.

7.1.2.3.2. Delayed Email Audit

The to-be-sent emails will be delayed for audit. Only when they have been audited will they be sent.

The configuration page is as shown below:


Edit Access Control Policy
Help
Single policy
Multiple policies
Description:
Expiry Date:
Never expire
Expired on
Status:
Enable
Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
Enable Email Filter
Send/Receive Mail
Delayed Email Audit
Enable Delayed Email Audit
Audit Address List (Emails sent to the following addresses or suffixes will be delayed for audit before they are sent out)
Note: "abc.com" includes "abc.com" and "abc.com.cn". If "abc.com" is entered here, the emails addressed to "abc.com" or "abc.com.cn" will be audited before they are sent out.
The email whose SMTP authentication password contains less than 3 characters cannot be sent out after being audited.
Audit-free Address List (Emails sent to the following addresses or suffixes will not be audited.)
Note: "abc.com" includes "abc.com" and "abc.com.cn". If "abc.com" is entered here, the emails addressed to "abc.com" or "abc.com.cn" will not be audited.
Mail size > 0 K
Attachment number > 0
Email contains the following keywords in title or content
Note: Regular expression is supported. For example, "key.*d" will match "keyd" and "keyword".
Set administrator email address for this policy:
OK
Cancel

[Audit Address], [Audit-free Address List]: Define respectively the email address(es) to be audited or not to be audited.

For instance, if you do not want to audit the emails received by the email addresses of the enterprise itself, you can type the domain name of the enterprise' Mail Server in [Audit-free Address List] text box, such as *@vpn.com.cn.* This configuration will free the email addresses from delay and audit whose suffix is *@vpn.com.cn.*

Except the above settings, you can also define the [Mail size] and [Attachment number] of the emails that should be audited.

[Email contains the following keywords in title or content]: Configures the keyword that may be contained in the email title or content. The emails whose title or content contains the any of the keywords configured in the list will be delayed and audited.

For instance, type the keyword "source code" in the text box, and the email will be delayed from being sent if its title or content contains this keyword.

[Set administrator email address for this policy]: Configures the auditor's email address if there is

any email need audit. The audit information will be automatically delivered to this email address if there is email need audit. Check and configure this item to avoid delaying the delivery of some important emails. This function must be in association with he configurations in [Advance] > [Alarm] page. For details, please refer to Section 12.1 Alarm.

- [Email Filter] is only valid for SMTP and POP3 protocol, but invalid for WEBMAIL.
- Length of the [SMTP Server Address] authentication must not be shorter than 3 characters; otherwise, the audited emails will fail to be audited.

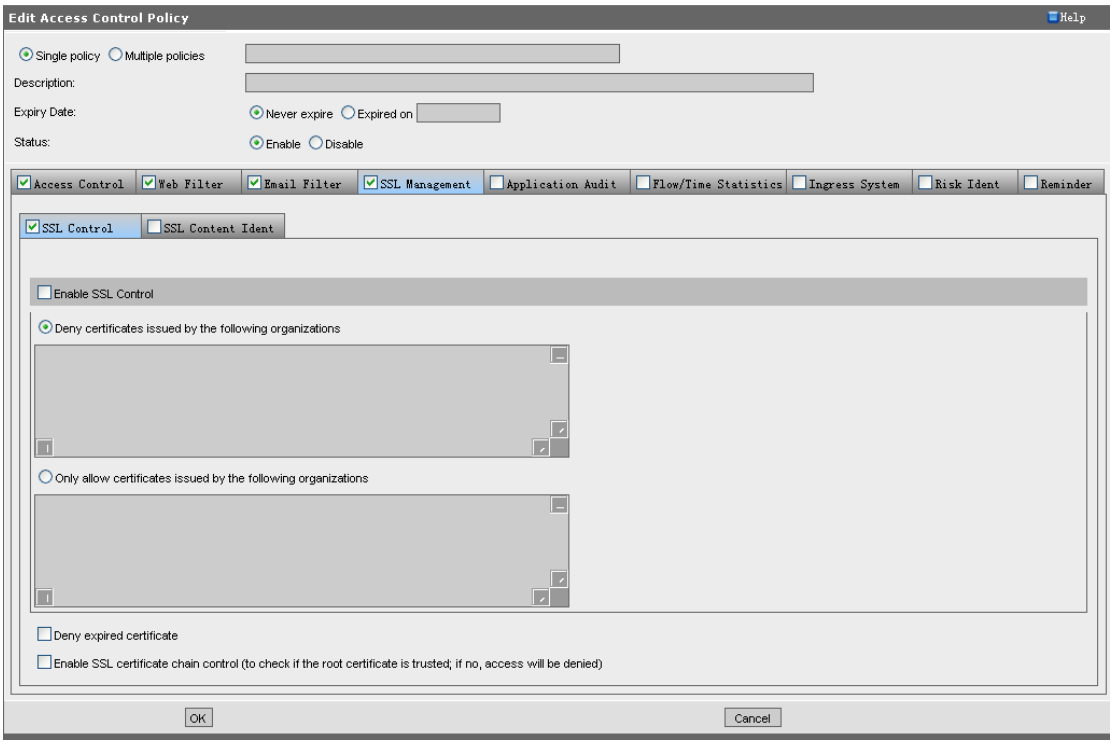
7.1.2.4. SSL Management

[SSL Management] controls the LAN users to visit certain websites, with the help of the black list and white list and the configuration whether to allow expired certificate. This function can further enhance the security level of SSL access (for it can apply the black list and white list, deny expired certificate, and verify the certificate chain). [SSL Management] covers the configuration of [SSL Control] and [SSL Content Ident].

7.1.2.4.1. SSL Control

[SSL Control]: Check this item to activate the function.

The configuration page is as shown below:



[Enable SSL Control]: Check this item to enable the [SSL black/white list control] function.

Type the black list and white list respectively in the corresponding text box; and configure whether to enable the expired certificate.

[Deny certificates issued by the following organizations]: Defines the certificate issuer of the website which is denied to be accessed. This is what is called as the “Black List”.

[Only allow certificates issued by the following organizations]: Defines the certificate issuer of the website which is allowed to be accessed. This is what is called as the “White list”.

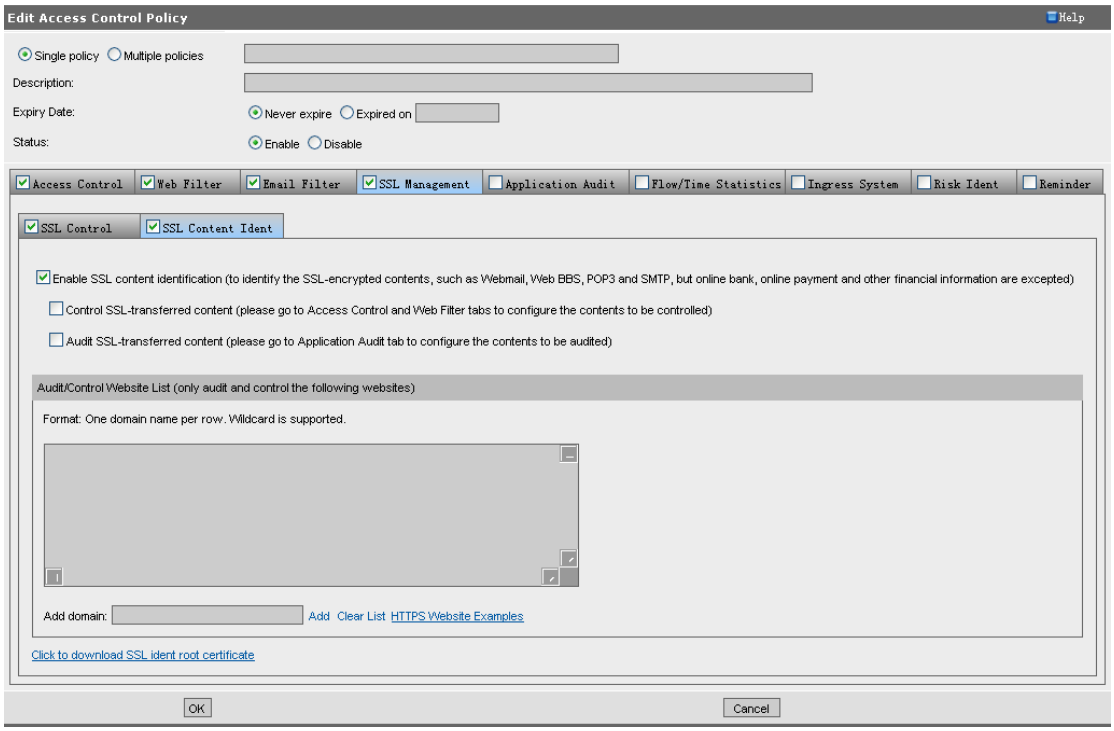
[Deny expired certificate]: Check this item and it will verify whether the certificate has expired. If it has expired, the LAN user then cannot access this website.

[Enable SSL certificate chain control] is used for verifying the certificate chain according to the trusted root certificates listed in [Object] > [SSL certificate] page. If the sub CA is not coherent to the root CA, or the certificate has been altered during the issuing process, the LAN computer will be denied to get access to the Internet.

7.1.2.4.2. SSL Content Ident

[SSL Content Ident] can identify the SSL-encrypted WEBMAIL, WEB-BBS, POP3 and SMTP contents (financial services such as online banking and online payment are excluded).

[SSL Content Ident]: Check this item to activate the SSL content identification function. The configuration page is as shown below:


Edit Access Control Policy
Help
Single policy
Multiple policies
Description:
Expiry Date:
Never expire
Expired on
Status:
Enable
Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
SSL Control
SSL Content Ident
Enable SSL content identification (to identify the SSL-encrypted contents, such as Webmail, Web BBS, POP3 and SMTP, but online bank, online payment and other financial information are excepted)
Control SSL-transferred content (please go to Access Control and Web Filter tabs to configure the contents to be controlled)
Audit SSL-transferred content (please go to Application Audit tab to configure the contents to be audited)
Audit/Control Website List (only audit and control the following websites)
Format: One domain name per row. Wildcard is supported.
Add domain:
Add
Clear List
HTTPS Website Examples
Click to download SSL ident root certificate
OK
Cancel

[Enable SSL content identification]: Check this item to enable the identification function, and the SSL-encrypted WEBMAIL, WEB-BBS, POP3, SMTP contents will be identified, excluding financial services such as online banking, online payment, etc.

[Audit/Control Website List (only audit and control the following websites)]: This function is only available when [Enable SSL content identification] is checked. You have to add the domain name of the website whose SSL-encrypted contents are to be audited or controlled, one entry (domain name) per row. If it is left blank, no SSL application will be identified.

[Control SSL-transferred content]: Check this option and the SSL objects will be controlled. As to the detailed items to be controlled, please configure them in the [Access Control Policy] > [Edit Access Control Policy] page > [Access Control] and [Web Filter].

[Audit SSL-transferred content]: Check this option and the identified SSL objects will be audited. As to the detailed items to be audited, please configure them in [Access Control Policy] > [Edit Access Control Policy] page > [Application Audit].

<Click to download SSL ident root certificate>: Click this link to download the legal SSL certificates, so as to eliminate the security alarm caused by enabling [SSL content identification] function.

SSL content identification function is invalid for financial services, such as online banking, online payment, etc.

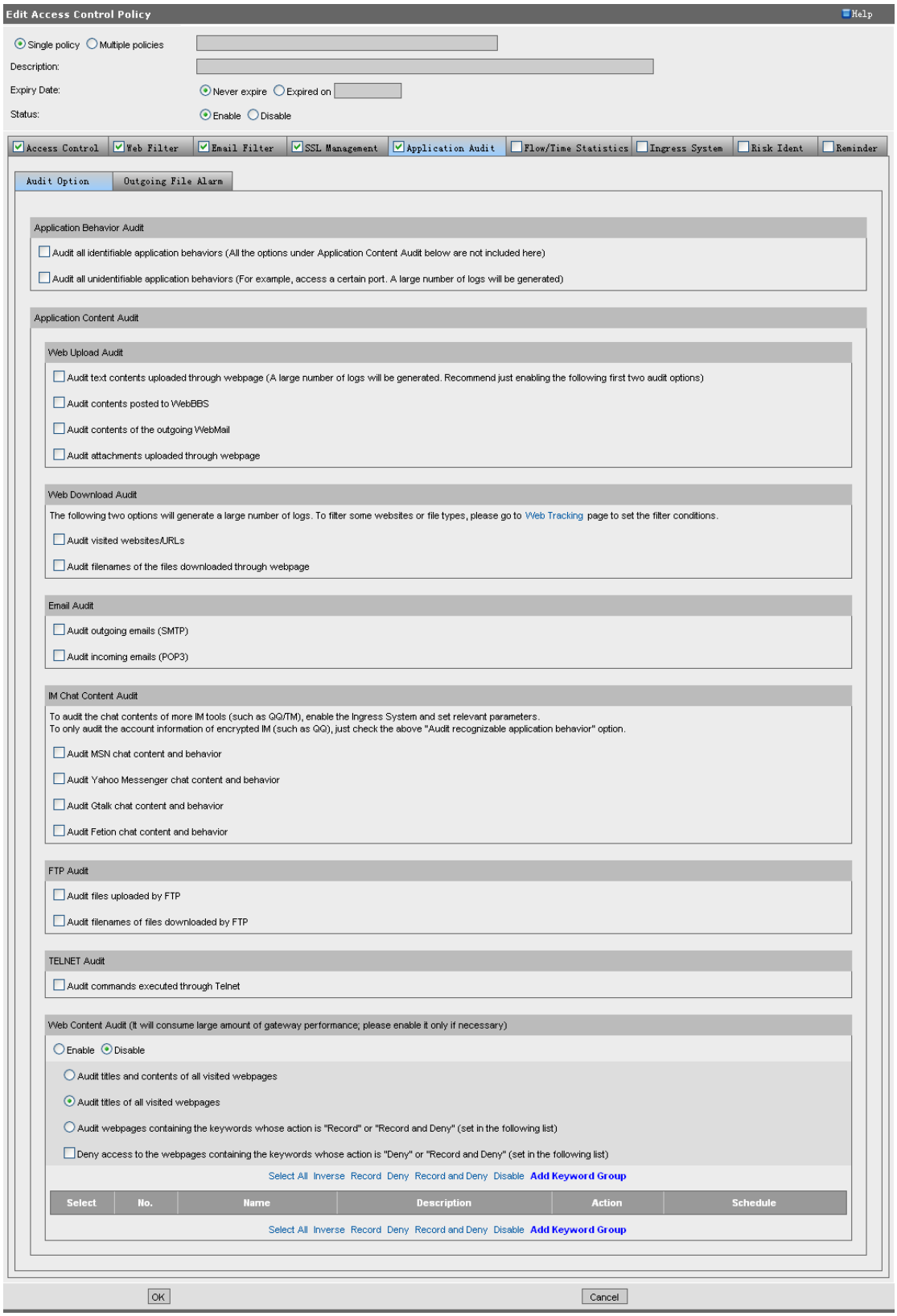
7.1.2.5. Application Audit

[Application Audit] helps monitoring the Internet access information and records of the LAN users, including configuration of [Audit Option] and [Outgoing File Alarm].

7.1.2.5.1. Audit Option

[Audit Option]: Check this option to activate the configurations under it.

The configuration page is as shown below:


Edit Access Control Policy
Help
Single policy
Multiple policies
Description:
Expiry Date:
Never expire
Expired on
Status:
Enable
Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
Audit Option
Outgoing File Alarm
Application Behavior Audit
Audit all identifiable application behaviors (All the options under Application Content Audit below are not included here)
Audit all unidentifiable application behaviors (For example, access a certain port. A large number of logs will be generated)
Application Content Audit
Web Upload Audit
Audit text contents uploaded through webpage (A large number of logs will be generated. Recommend just enabling the following first two audit options)
Audit contents posted to WebBBS
Audit contents of the outgoing WebMail
Audit attachments uploaded through webpage
Web Download Audit
The following two options will generate a large number of logs. To filter some websites or file types, please go to Web Tracking page to set the filter conditions.
Audit visited websites/URLs
Audit filenames of the files downloaded through webpage
Email Audit
Audit outgoing emails (SMTP)
Audit incoming emails (POP3)
IM Chat Content Audit
To audit the chat contents of more IM tools (such as QQ/TM), enable the Ingress System and set relevant parameters.
To only audit the account information of encrypted IM (such as QQ), just check the above "Audit recognizable application behavior" option.
Audit MSN chat content and behavior
Audit Yahoo Messenger chat content and behavior
Audit Gtalk chat content and behavior
Audit Fetion chat content and behavior
FTP Audit
Audit files uploaded by FTP
Audit filenames of files downloaded by FTP
TELNET Audit
Audit commands executed through Telnet
Web Content Audit (It will consume large amount of gateway performance; please enable it only if necessary)
Enable
Disable
Audit titles and contents of all visited webpages
Audit titles of all visited webpages
Audit webpages containing the keywords whose action is "Record" or "Record and Deny" (set in the following list)
Deny access to the webpages containing the keywords whose action is "Deny" or "Record and Deny" (set in the following list)
Select All Inverse Record Deny Record and Deny Disable Add Keyword Group
Select
No.
Name
Description
Action
Schedule
Select All Inverse Record Deny Record and Deny Disable Add Keyword Group
OK
Cancel

[Audit Option] falls into the following aspects:

[Application Behavior Audit]: Records all the behaviors of the LAN users on the Internet.

[Application Content Audit]: Audits the contents of the specific applications used by the LAN users.

[Web Upload Audit]: Audits the text contents, BBS posting contents, WebMail contents and the contents of the attachments that the LAN users are to upload.

[Web Download Audit]: Audits the website of the webpage that the LAN users are going to visit and the file name downloaded from webpage.

[Email Audit]: Audits all the email information received or sent through SMTP or POP3.

[IM Chat Content Audit]: Audits the chat contents and behaviors through IM software such as MSN, Yahoo Messenger, GTALK and Fetion, etc.

[FTP Audit]: Audits the file names of the files uploaded or downloaded through FTP.

[Telnet Audit]: Audit the commands executed by the LAN users through Telnet.

[Web Content Audit]: Audit the title and content body of the webpage. It is only applicable to the webpage containing the configured keyword(s).

[Enable], [Disable]: Select it to enable or disable the audit function over web content. The audited items fall into, [Audit titles and contents of all visited webpages], [Audit titles of all visited webpages] and [Audit webpages containing the keywords whose action is "Record" or "Record and Deny"]

[Deny access to the webpages containing the keywords whose action is "Deny" or "Record and Deny"]: Check this option to deny the webpage access if the webpage contains the keywords whose action is "Deny" or "Record and Deny".

Select the needed item; add the keyword group, and select the corresponding [Action] and [Schedule]. As to the configuration of keywords, please refer to Section 7.1.2.2.3 (under [IAM] > [Access Control Policy] > [Edit Access Control Policy] page > [Web Filter]).

Having completed configuring this page, you have to click the <OK> button to save all the settings.

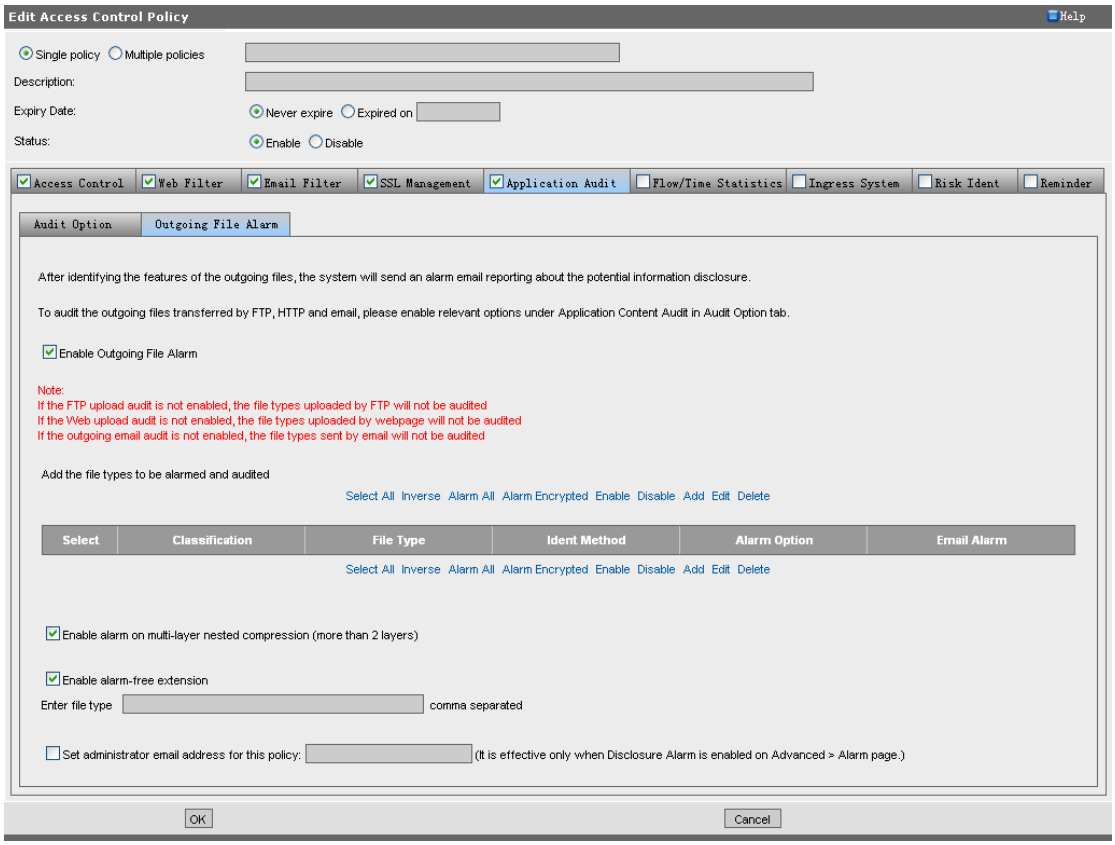
The application audit records are stored in the Data Center. You can search the records in [Internet Access Audit] > [Enter Data Center].

- The emails delivered through WebMail and the BBS posts can only be displayed under certain decoding.
- Checking [Web Content Audit] will lead to massive logs. If you do not want some websites or file types to be audited, please configure the options in [Advanced] > [Web Tracking].
- Name of the attachments sent or received through MSN or Yahoo Messenger can be recorded. If you want to only audit the encrypted IM accounts such as QQ, check [Application Audit] > [Audit all identifiable application behaviors (All the options under Application Content Audit below are not included here)].
- If you want to record the chat content details through the encrypted IM software, you have to configure a corresponding ingress rule. As to the detailed introduction to ingress rule, please refer to Section 7.1.2.7 Ingress System.

7.1.2.5.2. Outgoing File Alarm

[Outgoing File Alarm] configurations help to identify the features of the outgoing files and give audit alarm, so as to prevent information disclosure.

Check [Application Audit] and then check [Outgoing File Alarm], the pop-up configuration page appears, as shown below:


Edit Access Control Policy
Help
Single policy
Multiple policies
Description:
Expiry Date:
Never expire
Expired on
Status:
Enable
Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
Audit Option
Outgoing File Alarm
After identifying the features of the outgoing files, the system will send an alarm email reporting about the potential information disclosure.
To audit the outgoing files transferred by FTP, HTTP and email, please enable relevant options under Application Content Audit in Audit Option tab.
Enable Outgoing File Alarm
Note:
If the FTP upload audit is not enabled, the file types uploaded by FTP will not be audited
If the Web upload audit is not enabled, the file types uploaded by webpage will not be audited
If the outgoing email audit is not enabled, the file types sent by email will not be audited
Add the file types to be alarmed and audited
Select All Inverse Alarm All Alarm Encrypted Enable Disable Add Edit Delete
Select
Classification
File Type
Ident Method
Alarm Option
Email Alarm
Select All Inverse Alarm All Alarm Encrypted Enable Disable Add Edit Delete
Enable alarm on multi-layer nested compression (more than 2 layers)
Enable alarm-free extension
Enter file type
comma separated
Set administrator email address for this policy:
(It is effective only when Disclosure Alarm is enabled on Advanced > Alarm page.)
OK
Cancel

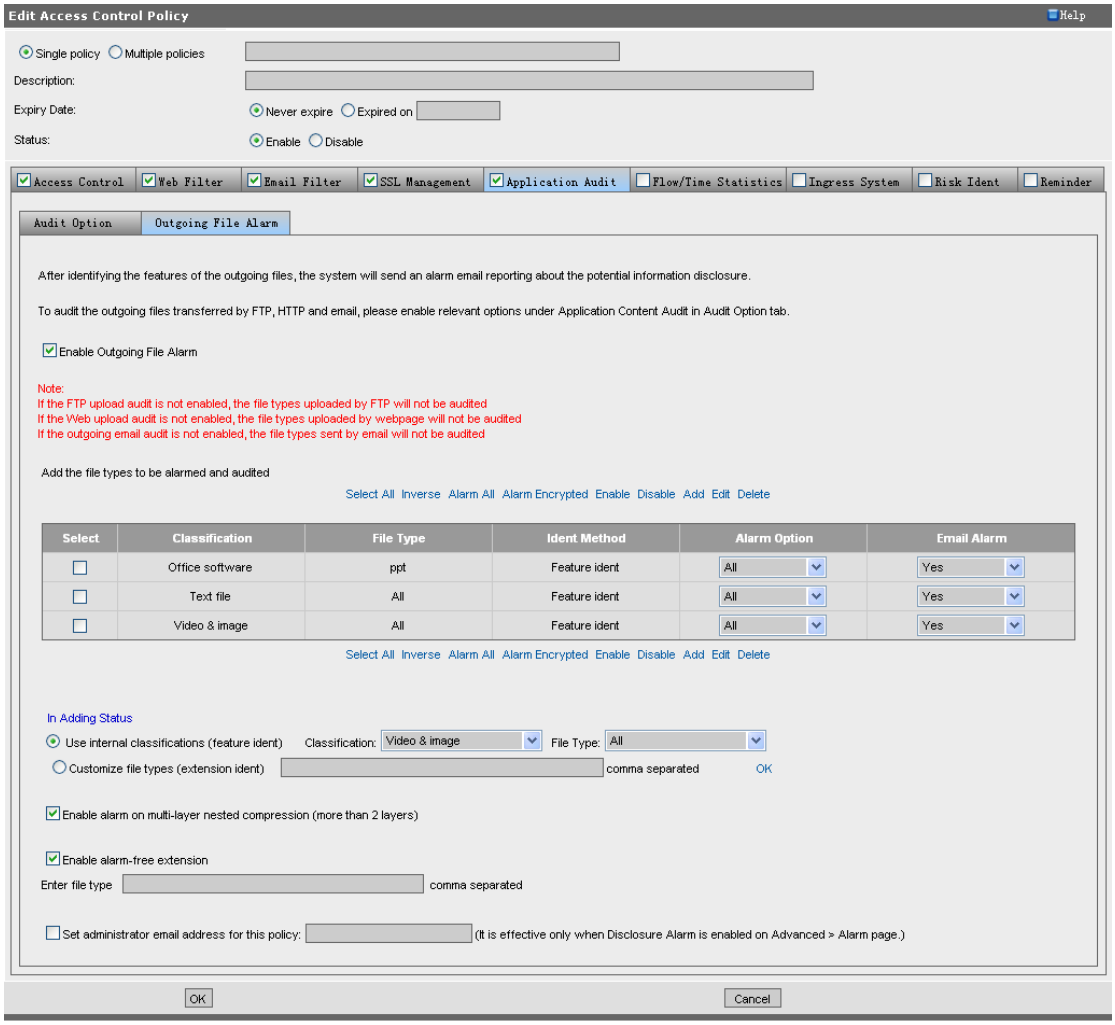
[Enable Outgoing File Alarm]: Check this option to activate the outgoing file alarm function.

<Select All>, <Inverse>: Click it (above/below the file type list) to select the needed file type(s).

<Alarm All>, <Alarm Encrypted>: Click it (above/below the file type list) to configure the [Alarm Option] of the selected file type(s).

<Enable>, <Disable>: Click it (above/below the file type list) to configure whether to give [Email Alarm] to notify the administrator while the configured file type(s) is detected.

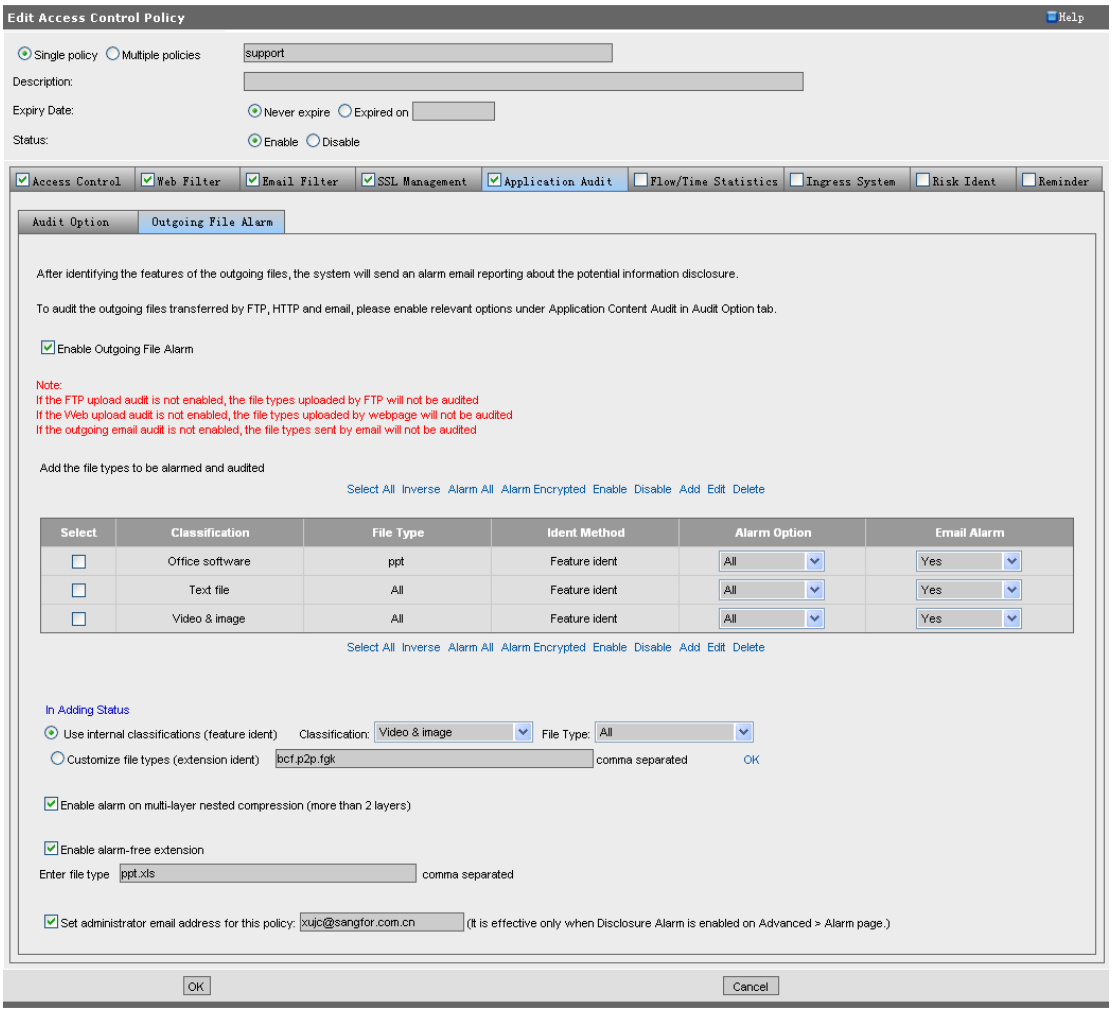
<Add>: Click it (above/below the file type list) and configure a new file type to add this new file type into the list, as shown below:



[In Adding Status]: Configures the option under it. You can configure the new file type here.

[Use internal classifications (feature ident)]: Select a file type from the existing internal library and then click <OK>. The access control policy will identify the application according to the features of this specific file type.

[Customize file types (extension ident)]: Type the file type name in the text box and click <OK>. The access control policy will identify the application according to the suffix of the file. You can enter several suffixes which are separated from each other with an English comma (,).



[Enable alarm on multi-layer nested compression (more than 2 layers)]: Check this option and it will give alarm when the nested compression file is detected.

[Enable alarm-free extension]: Check this option and enter the file type(s) free from alarm. You can type several suffixes in the text box which are separated from each other with an English comma (,).

[Set administrator email address for this policy]: Check this option and type the receiver of the alarm emails. To successfully send the alarm emails to the administrator email address and notify the administrator of the alarm information, you have to configure the options in [Advanced] > [Alarm]. For detailed introduction to the configuration, please refer to Section 12.1 Alarm.

- [Outgoing File Alarm] is unavailable by default. If you want to activate this function, you

have to activate the corresponding license. As to the detailed operation, please refer to Section 3.3 License.

- To have the [Outgoing File Alarm] function work, you have to enable [Audit files uploaded by FTP], [Web Upload Audit] and [Audit outing emails], please refer to Section 7.1.2.5 Application Audit.
- For scanning a large alarm-free compressed file package, it only scans its 100 files and checks whether there are potential files that need alarm. If an alarm email is to be sent, this alarm email will contain the information of the first event that needs alarm. One log only records the detailed information of (at most) one file and the general alarm information of other file(s).
- If the outgoing file is delivered through email, its eml format attachment will be audited, and the email alarm will be delivered to the administrator email address.

7.1.2.6. Flow/Time Statistics

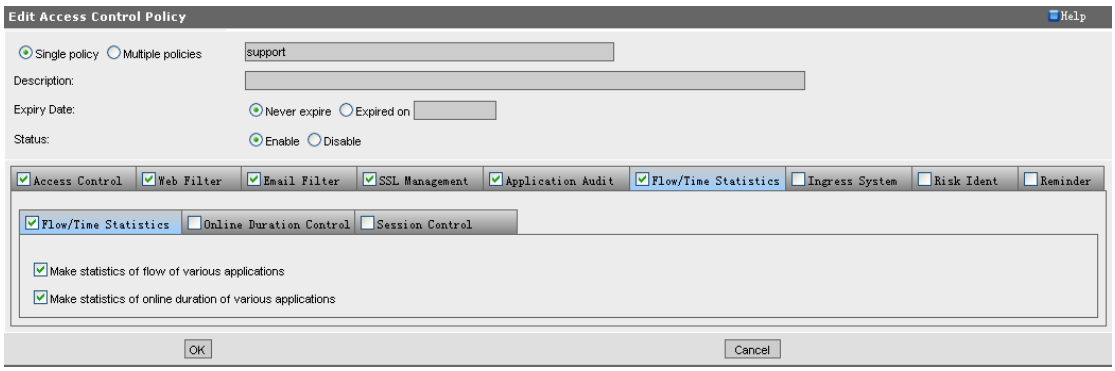
[Flow/Time Statistics] covers the configuration of [Flow/Time Statistics], [Online Duration Control] and [Session Control].

[Flow/Time Statistics]: Check this option to activate this function and the configurations under it.

7.1.2.6.1. Flow/Time Statistics

[Flow/Time Statistics] mainly makes statistics of the bandwidth/flow of various applications that are used by the user group, and the online time statistics of the users on these applications.

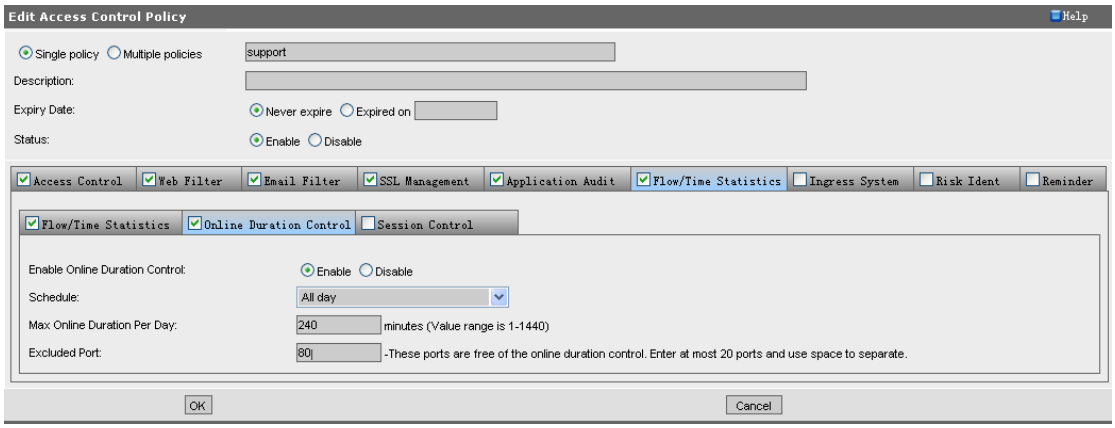
The configuration page is as shown below:



7.1.2.6.2. Online Duration Control

[Online Duration Control] configuration can control the online duration of the users.

The configuration page is as shown below:



[Enable Online Duration Control]: Select [Enable] or [Disable] to enable or disable this control function respectively.

[Schedule]: Select a time schedule during which the users can get access to the Internet through the IAM gateway device. As to the configuration of a schedule, please refer to Section 4.5 Schedule.

[Max Online Duration Per Day]: Configures the online duration, in unit of minute.

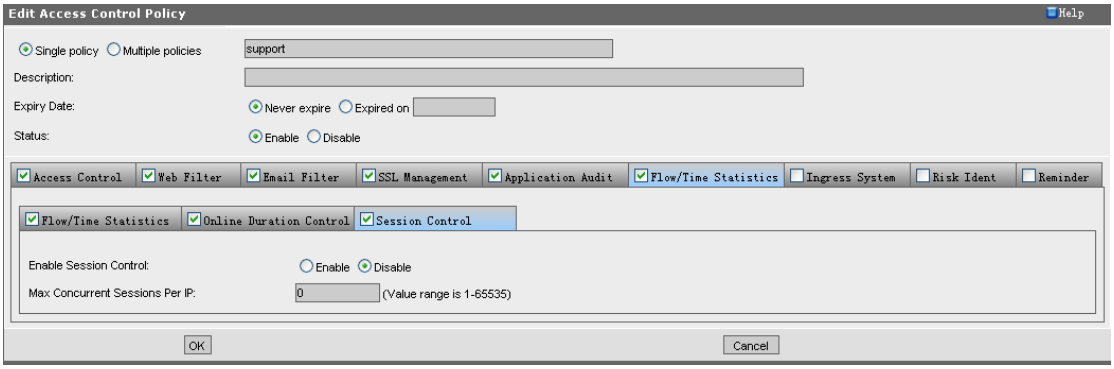
[Excluded Port]: Configures the port that is free from online duration control; the port filled in here should be target port.

Having completed configuring this page, you have to click the <OK> button to save the settings.

7.1.2.6.3. Session Control

[Session Control] configures the maximum sessions allowed for each IP address.

The configuration page is as shown below:



[Enable Session Control]: Enable it to limit the maximum concurrent sessions (connections) for a single IP address (user). This function can prevent the users from creating large number of sessions caused by scanning tool or using several download tools (at the same time) such as P2P. It helps to lower down the possibility that the viruses spread widely by scanning and connecting to other devices.

[Max Concurrent Sessions Per IP]: Configures the maximum concurrent sessions for a single IP address. If the number of concurrent connections of a single IP address reaches the threshold configured here, the session (connection) request will be denied.

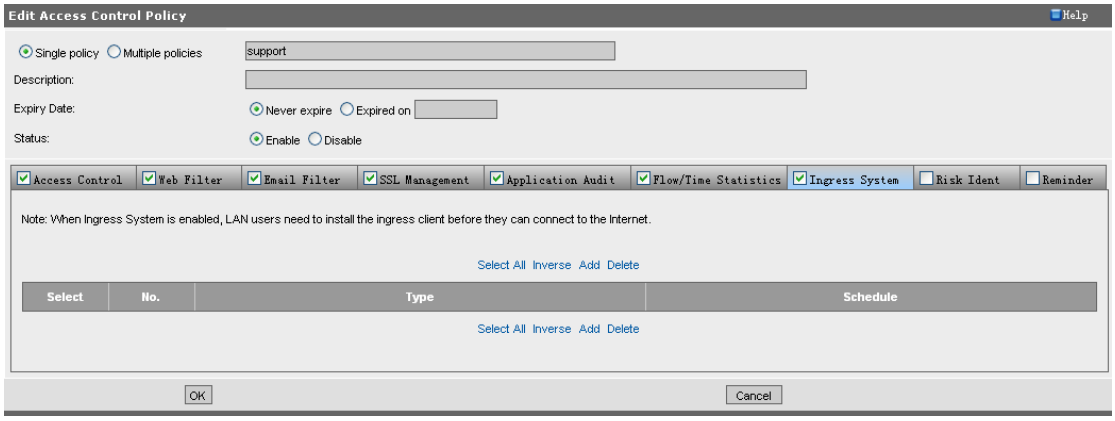
Having completed configuring this page, you have to click the <OK> button to save the settings.

7.1.2.7. Ingress System

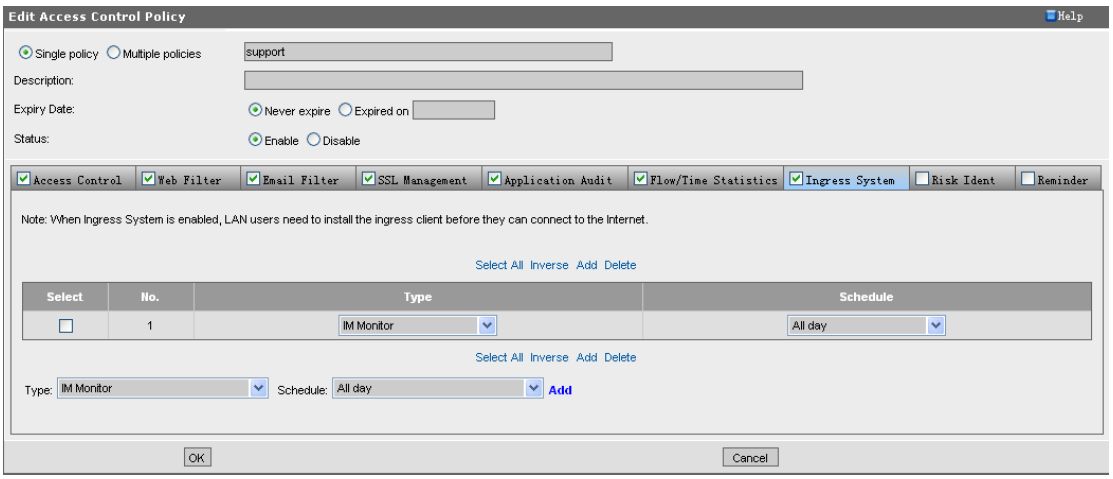
[Ingress System] is used for banning the use of proxy software, inspecting the status of binding IP/MAC over the layer 3 switch and monitoring encrypted IM message, etc. If the access control policy has applied the ingress rule(s), the user' computer has to satisfy the corresponding rules configured on IAM gateway device to get access to the Internet. As to the configuration of ingress rule, please refer to Section 4.10 Ingress Rule.

[Ingress System]: Check this item to activate the ingress rule.

The configuration page is as shown below:



<Add>: Click this button and the options pop up, as shown below:



Select a [Type], [Schedule] and then click the <Add> to add this new ingress rule into the list. As to the configuration of a new schedule (here it indicates the valid time), please refer to Section 4.5 Schedule.

<Select All>, <Inverse>: Click it (above/below the list) to select the needed ingress rule(s).

<Delete>: Click it to delete the selected ingress rule(s).

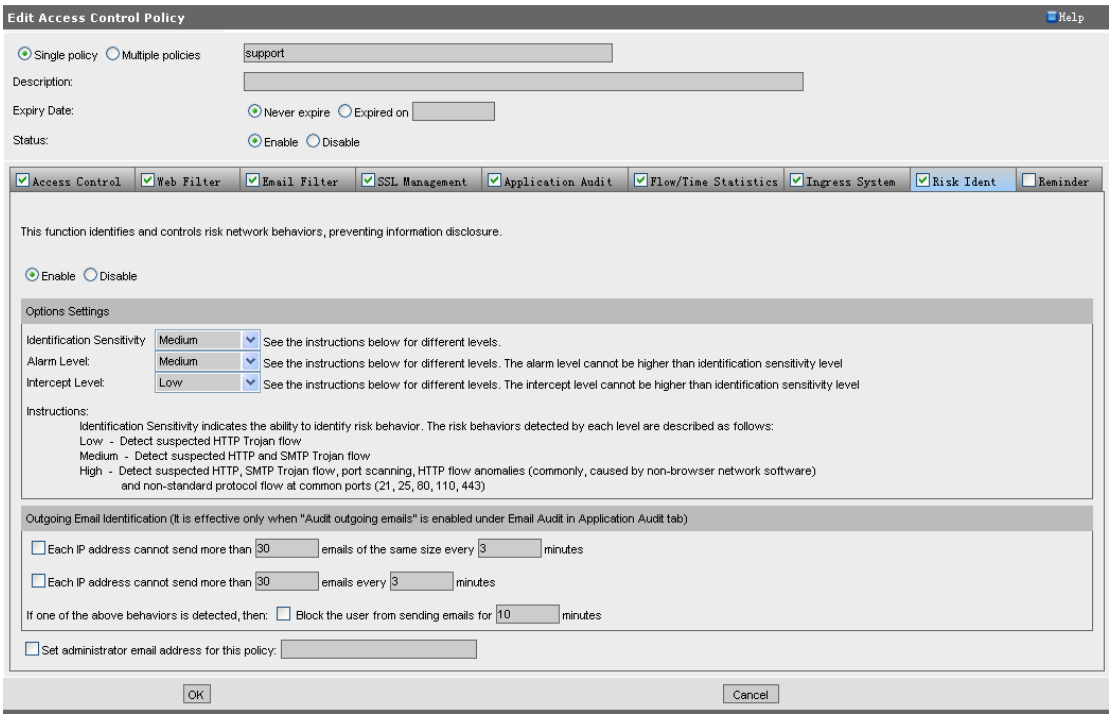
Having completed configuring this page, you have to click the <OK> button to save the settings.

7.1.2.8. Risk Ident

[Risk Ident] is used for identifying and controlling risky behaviors of the users, so as to prevent the information from being disclosed.

[Options Settings] configures the options to identify and control the traffic caused by HTTP Trojan, SMTP Trojan, port scanning, non-standard protocol transmission at common and well-known ports, and by suspicious HTTP applications.

[Risk Ident]: Check this item and the options pop up, as shown below:


Edit Access Control Policy
Help
Single policy
Multiple policies
support
Description:
Expiry Date:
Never expire
Expired on
Status:
Enable
Disable
Access Control
Web Filter
Email Filter
SSL Management
Application Audit
Flow/Time Statistics
Ingress System
Risk Ident
Reminder
This function identifies and controls risk network behaviors, preventing information disclosure.
Enable
Disable
Options Settings
Identification Sensitivity
Medium
See the instructions below for different levels.
Alarm Level:
Medium
See the instructions below for different levels. The alarm level cannot be higher than identification sensitivity level
Intercept Level:
Low
See the instructions below for different levels. The intercept level cannot be higher than identification sensitivity level
Instructions:
Identification Sensitivity indicates the ability to identify risk behavior. The risk behaviors detected by each level are described as follows:
Low - Detect suspected HTTP Trojan flow
Medium - Detect suspected HTTP and SMTP Trojan flow
High - Detect suspected HTTP, SMTP Trojan flow, port scanning, HTTP flow anomalies (commonly, caused by non-browser network software) and non-standard protocol flow at common ports (21, 25, 80, 110, 443)
Outgoing Email Identification (It is effective only when "Audit outgoing emails" is enabled under Email Audit in Application Audit tab)
Each IP address cannot send more than 30 emails of the same size every 3 minutes
Each IP address cannot send more than 30 emails every 3 minutes
If one of the above behaviors is detected, then: Block the user from sending emails for 10 minutes
Set administrator email address for this policy:
OK
Cancel

[Enable], [Disable]: Select it to enable or disable the risky behavior identification function.

[Identification Sensitivity]: Configures the sensitivity level of the rule detecting risky behaviors. Options are [High], [Medium] and [Low].

[Alarm Level]: Configures the alarm priority of the identified risky behaviors; options are [High], [Medium], [Low] and [Disable].

[Intercept Level]: Configures the measure (interception) level taken when risky behavior is identified; options are [High], [Medium], [Low] and [Disable].

[Outgoing Email Identification]: Configures the options to identify and block outgoing email anomaly. Identification can be based on the number of same-sized emails sent by a single IP address in certain time period, and frequency of the emails sent by a single IP address in a certain time period, etc.

[Set administrator email address for this policy]: Configure the email address of the administrator to which the alarm emails are delivered when risky behavior is detected.

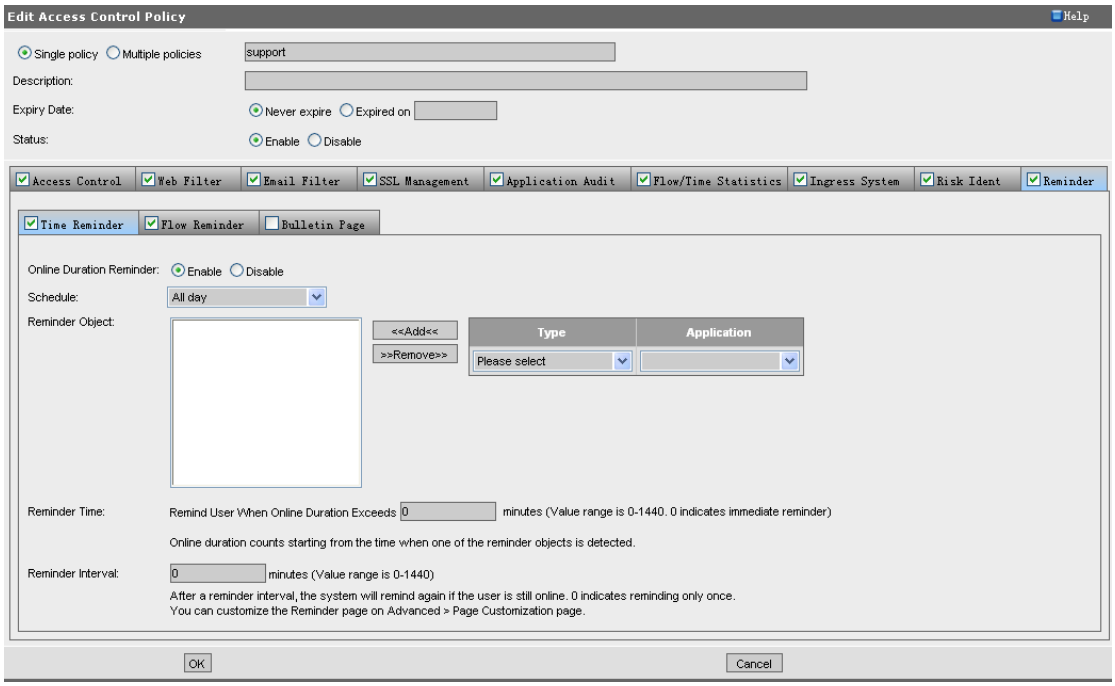
To have the administrator receive the email notice that risky behavior is detected, you have to configure the corresponding options in [Advanced] > [Alarm] page. For detailed configuration, please refer to Section 12.1 Alarm.

- [Risk Ident] function is disabled by default. If you want to activate this function, you have to activate the corresponding license. As to the detailed operation, please refer to Section 3.3 License.
- [Alarm Level] and [Intercept Level] must not be higher than [Identification Sensitivity].
- To have [Outgoing Email Identification] function work, you have to enable [Email Audit] and configure the corresponding options. For details, please refer to Section 7.1.2.5 Application Audit.

7.1.2.9. Reminder

[Reminder] can warn the users of their behaviors, online time, flow and bulletin, etc. It covers the configurations of [Time Reminder], [Flow Reminder] and [Bulletin Page].

7.1.2.9.1. Time Reminder



[Online Duration Reminder]: Enable it to have the IAM gateway device record the online duration

of the users and activate the prompt settings.

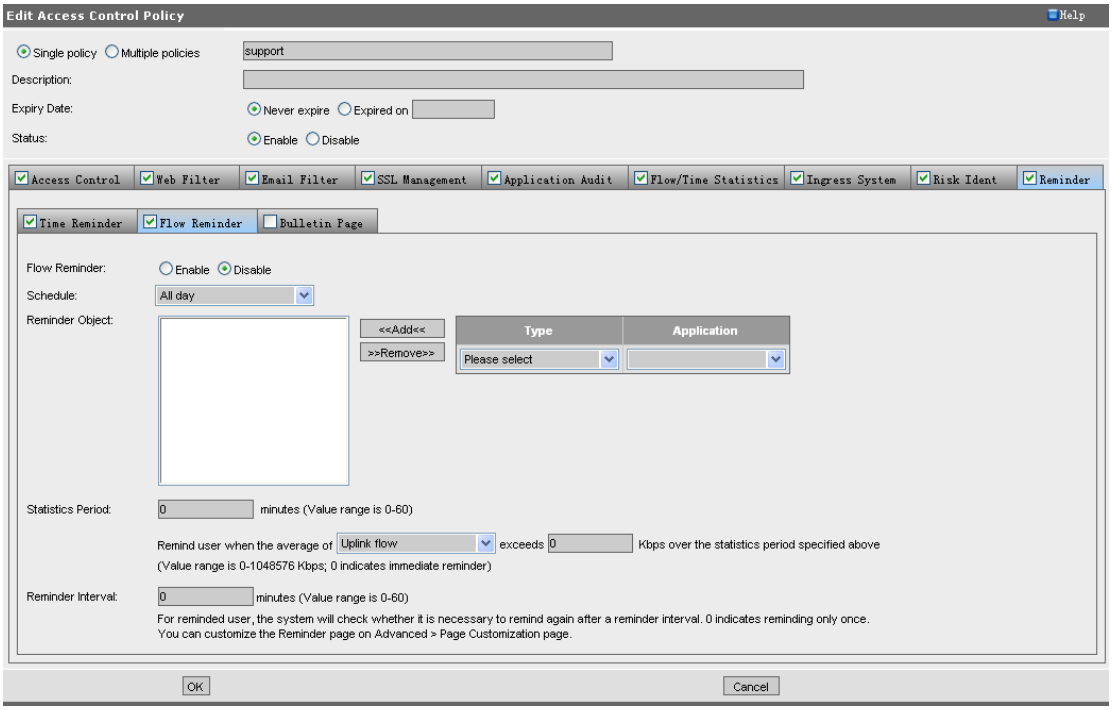
[Schedule]: Select the time period to define the valid time of the [Time Reminder] function. As to the configuration of a schedule, please refer to Section 4.5 Schedule.

[Reminder Object]: Configures the application type whose online time statistics is to be made. Only the online duration of the selected application types will be recorded. Detailed steps are: select an application type from the [Type] pull-down list and a specific application from [Application] pull-down list; and then click the <Add> button to add the application into the list; to remove a selected application from the list, just click the application and then click the <Delete> button.

[Reminder Time]: Configures the online time duration. If a user uses up the allowed online duration, the IAM gateway device will remind the user that it has used up the allocated online duration. Type a value ranging 0-1440 minutes. 0 indicates that the IAM gateway device will remind the user the moment it accesses the Internet.

[Reminder Interval]: Configures the interval that the user is reminded. If the user has been reminded once but it is still surfing on the Internet, the IAM gateway device will remind the user once again (or more) some time later (up to the configured [Reminder Interval]). Type a value ranging 0-1440; 0 indicates that the user will be reminded once.

7.1.2.9.2. Flow Reminder



[Flow Reminder]: Enable it to have the IAM gateway device record the online flow caused by the users and activate the prompt settings.

[Schedule]: Select the time period to define the valid time of the [Flow Reminder] function. As to the configuration of a schedule, please refer to Section 4.5 Schedule.

[Reminder Object]: Configures the application type whose online flow statistics is to be made. Only the online flow information of the selected application types will be recorded. Detailed steps are: select an application type from the [Type] pull-down list and a specific application from [Application] pull-down list; and then click the <Add> button to add the application into the list; to remove a selected application from the list, just click the application and then click the <Delete> button.

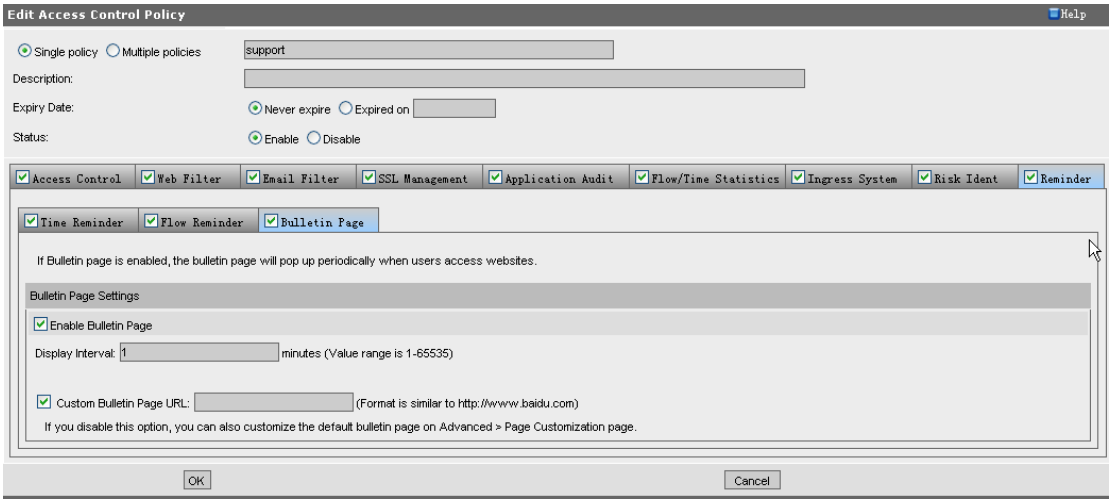
[Statistics Period]: Configures the time period during which the online flow caused by the user is to be averaged. If the averaged flow speed exceeds certain Kbps, the IAM gateway device will remind the user of it. Type a value (ranging 0-60) in the [Statistics Period] text box; 0 (but the averaged flow is not 0) indicates that the user will not be reminded. As to flow, you can define it as [Uplink flow], [Downlink flow] or [Total flow]. The averaged flow speed ranges 0-1Gbps. 0 indicates that the IAM gateway device will remind the user once flow caused by the selected applications is detected.

[Reminder Interval]: Configures the interval that the user is reminded of flow limit. If the user has been reminded once but the averaged flow speed still exceeds certain Kbps, the IAM gateway device will remind the user once again (or more) some time later (up to the configured [Reminder Interval]). Type a value ranging 0-1440; 0 indicates that the user will be reminded only once.

7.1.2.9.3. Bulletin Page

[Bulletin Page] defines the pop-up prompt page when the user visits a HTTP webpage for the first time.

[Enable Bulletin Page]: Check this option and the bulletin page will automatically pop up when the user visits a HTTP webpage for the first time (provided that the user has passed the authentication).



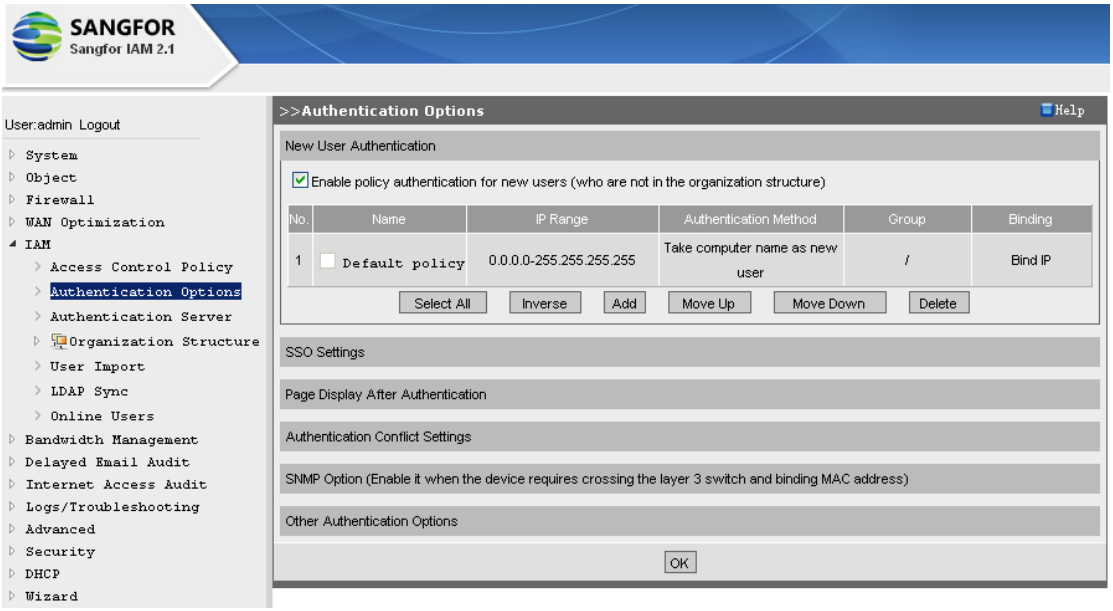
Having completed configuring this page, you have to click the <OK> button to save the settings.

- The related reminder pages can be defined and modified in [Advanced] > [Page Customization] page.
- In some rule modules (such as [Access Control], [Web Filter], etc.), there is a [Default Action] and an option [If several policies are associated, adopt the default action of the next policy and continue matching downwards]. If you DO NOT check the latter, the access control policy will apply the [Default Action] of the current control policy, instead of having the data packets continue to match the rules of the access control policies followed.
- In other rule modules, it takes the first rule as the final when matching the access control policy. These rule modules include [Access Control] > [Proxy Control], [SSL Management], [Email Filter], [Application Audit], [Flow/Time Statistics] and [Risk Ident].
- Generally speaking, the rules of a policy are matched from top to bottom. A rule will take effect once it is matched, and the next rule of the same type will not be matched once again. For this reason, it is recommended that the more detailed rules are the upper ones while the general rules are at the bottom of the rule list. If the detailed rules are involved in the general rules, logic error of rules being matched will occur. Please DO arrange the rules in a right order.

7.2. Authentication Options

[Authentication Options] mainly configures the IAM gateway device and user authentication related options.

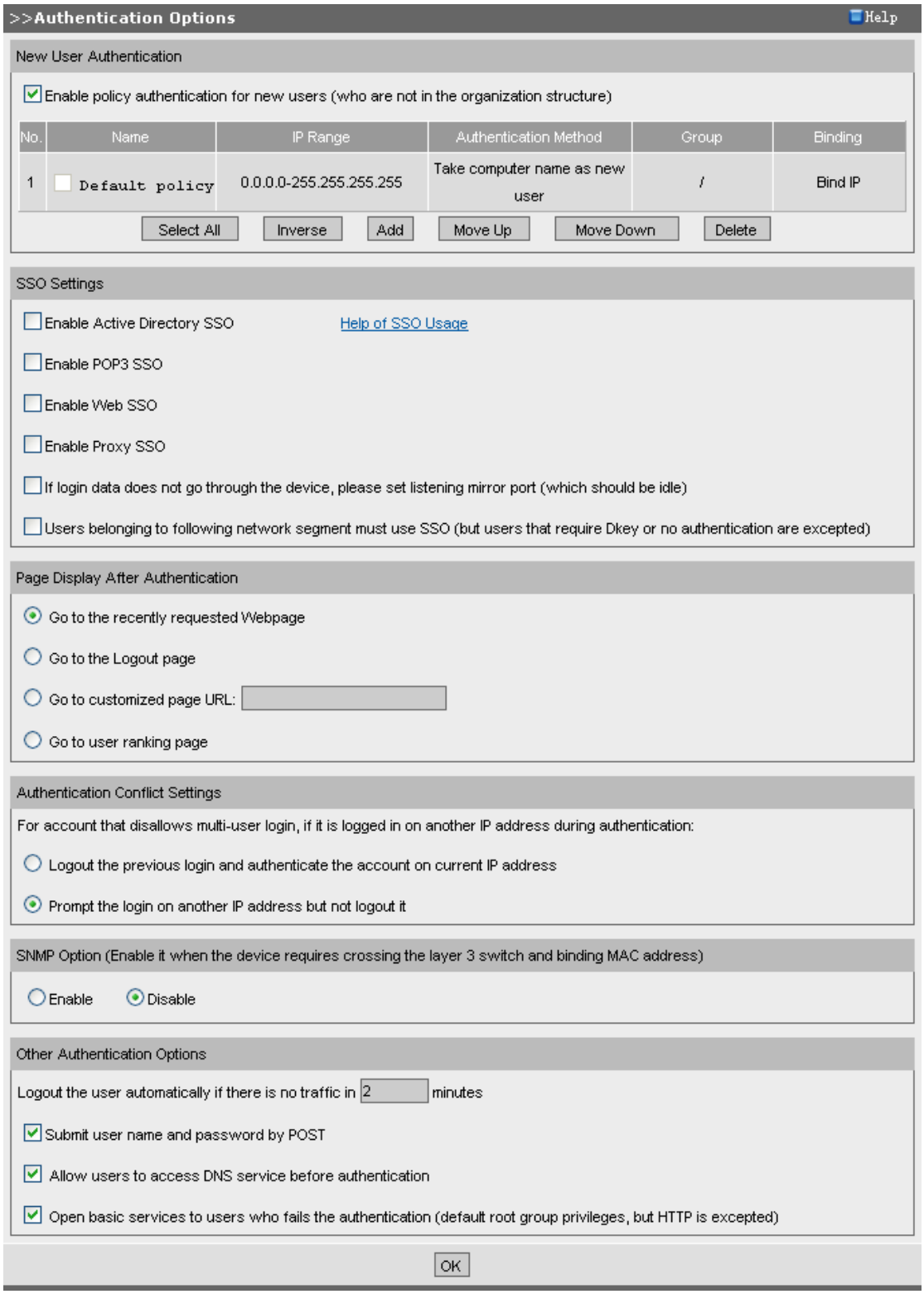
The configuration page is as shown below:



7.2.1. New User Authentication

[New User Authentication] configures the default policy that is applicable to the users not included in the member list. It can automatically add the new users to the member list and to certain group and bind the IP/MAC address of the user's.

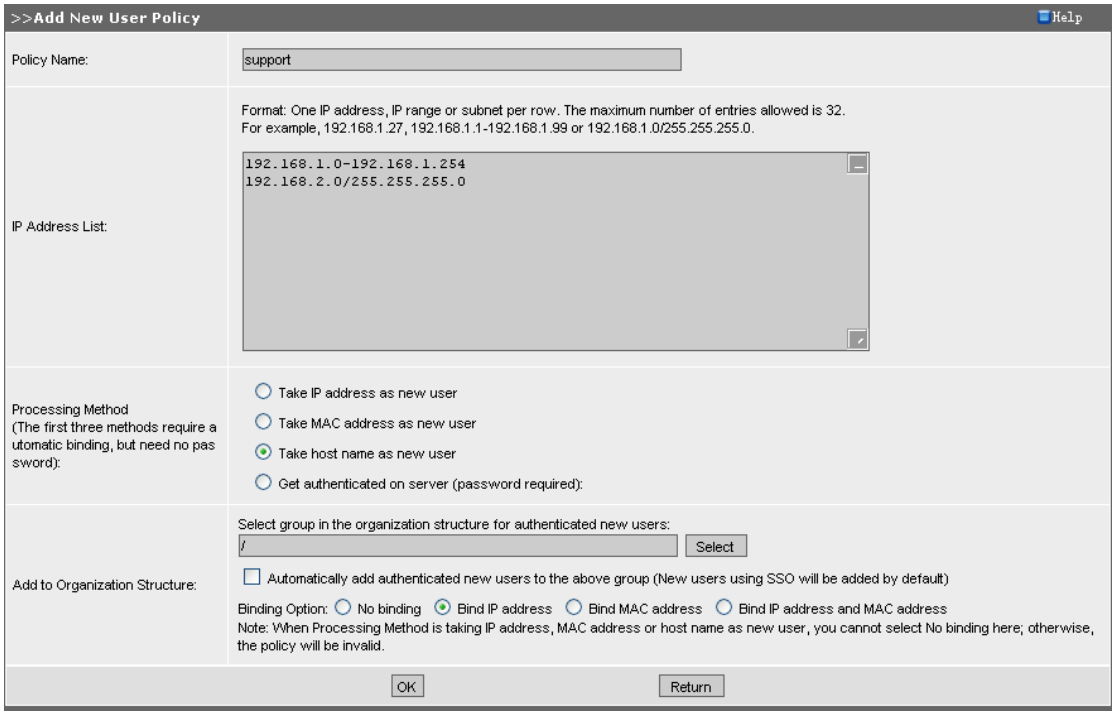
The configuration page is as shown below:


>>Authentication Options
Help
New User Authentication
Enable policy authentication for new users (who are not in the organization structure)
No.
Name
IP Range
Authentication Method
Group
Binding
1
Default policy
0.0.0.0-255.255.255.255
Take computer name as new user
/
Bind IP
Select All
Inverse
Add
Move Up
Move Down
Delete
SSO Settings
Enable Active Directory SSO
Help of SSO Usage
Enable POP3 SSO
Enable Web SSO
Enable Proxy SSO
If login data does not go through the device, please set listening mirror port (which should be idle)
Users belonging to following network segment must use SSO (but users that require Dkey or no authentication are excepted)
Page Display After Authentication
Go to the recently requested Webpage
Go to the Logout page
Go to customized page URL:
Go to user ranking page
Authentication Conflict Settings
For account that disallows multi-user login, if it is logged in on another IP address during authentication:
Logout the previous login and authenticate the account on current IP address
Prompt the login on another IP address but not logout it
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)
Enable
Disable
Other Authentication Options
Logout the user automatically if there is no traffic in 2 minutes
Submit user name and password by POST
Allow users to access DNS service before authentication
Open basic services to users who fails the authentication (default root group privileges, but HTTP is excepted)
OK

<Select All>, <Inverse>: Click it to select the needed new user policy.

<Move Up>, <Move Down>: Click it to move up or move down the selected new user policy.

<Add>: Click this button to add a new user policy.


>>Add New User Policy
Help
Policy Name:
support
Format: One IP address, IP range or subnet per row. The maximum number of entries allowed is 32.
For example, 192.168.1.27, 192.168.1.1-192.168.1.99 or 192.168.1.0/255.255.255.0.
IP Address List:
192.168.1.0-192.168.1.254
192.168.2.0/255.255.255.0
Processing Method
(The first three methods require a utomatic binding, but need no pas sword):
Take IP address as new user
Take MAC address as new user
Take host name as new user
Get authenticated on server (password required):
Add to Organization Structure:
Select group in the organization structure for authenticated new users:
/
Select
Automatically add authenticated new users to the above group (New users using SSO will be added by default)
Binding Option: No binding Bind IP address Bind MAC address Bind IP address and MAC address
Note: When Processing Method is taking IP address, MAC address or host name as new user, you cannot select No binding here; otherwise, the policy will be invalid.
OK
Return

[Name]: Type a name for this new user policy.

[IP Address List]: Configures the IP address(es) to which this new user policy is applicable. Only when the user whose IP address is any of the IP address in the list will it be matched by this policy.

Handling methods to a new user are:

[Take IP address as new user]: Automatically add the new user to the user list, taking the IP address of this user as its user name.

[Take MAC address as new user]: Automatically add the new user to the user list, taking the MAC address of this user as its user name.

[Take host name as new user]: Automatically add the new user to the user list, taking the host name of this user as its user name.

[Get authenticated on server (password required)]: Authentication is made through the third-party authentication server which requires user name and password. If the user name authenticated by the third-party server is not any of the users in the user list, this user will be automatically added to the assigned organization structure if [Automatically add authenticated new users to the above group] option is checked; or this user will exist as a casual user if the [Automatically add authenticated new users to the above group] option is not checked.

SANGFOR IAM gateway device supports the following third-party servers: LDAP server, RADIUS server and POP3 server.

You can choose the needed one according to your case. As to the configuration of third-party authentication server, please refer to Section 7.3 Authentication Server.

[Add to Organization Structure]: Check the option [Automatically add authenticated new users to the above group], and the applicable new users will be added to the assigned structure group and entitled with all the privileges of this structure group.

Except the above configurations, you can have the successfully-authenticated new users' IP address, MAC address, or both the IP and MAC address automatically bound; or neither of the IP or MAC address automatically bound.

- Enabling policy authentication for new users can have the IP addresses of different segments get authenticated differently, and add the user to the corresponding user group, and apply its individual access control policy.
- Taking the IP address as user name or taking host name as the user name requires the IAM gateway device binding at least with one IP address or MAC address of the user.
- If the IAM gateway device fails to resolve the host name because of the existence of the firewall on the client side, this host will be not added to the user list, but it will be entitled with all the privileges of its root group or the assigned user group (if it had been successfully added to certain user group).

7.2.2. SSO Settings

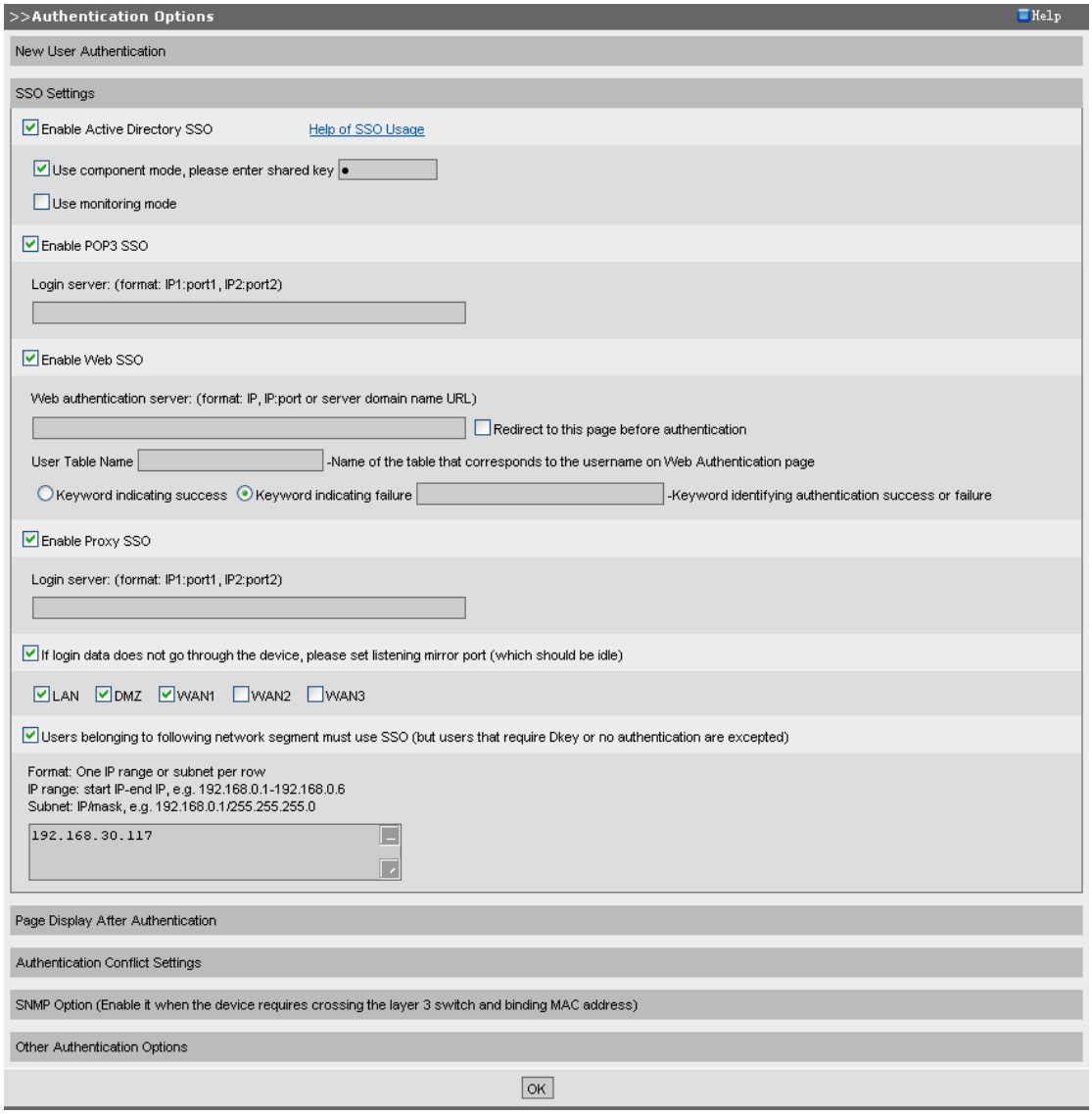
Single Sign-On (SSO) will not require the user for username and password once again after its first logon, but have the user automatically get passed when it logs in to the third-party authentication server.

The user need type only once the login password to log in to the third-party authentication server, automatically passing the authentication instead of typing password once again next time; therefore, it can lower the risk of password being disclosed.

[SSO Settings] covers the options for single sign-on, including POP3 SSO, Web SSO and Proxy

SSO, as well as the configuration of a listening port to listen to the login data of the network.

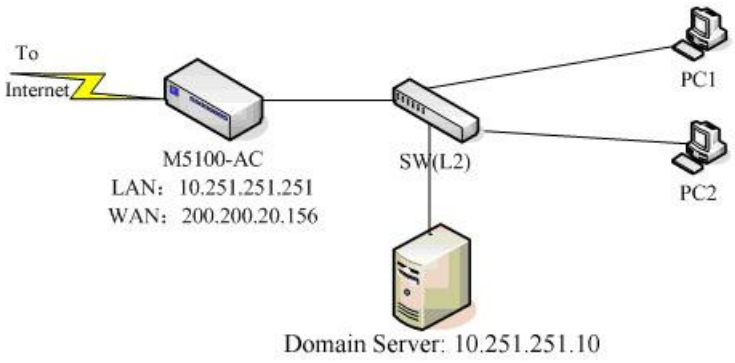
The configuration page is as shown below:


>>Authentication Options
Help
New User Authentication
SSO Settings
Enable Active Directory SSO
Help of SSO Usage
Use component mode, please enter shared key
Use monitoring mode
Enable POP3 SSO
Login server: (format: IP1:port1, IP2:port2)
Enable Web SSO
Web authentication server: (format: IP, IP:port or server domain name URL)
Redirect to this page before authentication
User Table Name
-Name of the table that corresponds to the username on Web Authentication page
Keyword indicating success
Keyword indicating failure
-Keyword identifying authentication success or failure
Enable Proxy SSO
Login server: (format: IP1:port1, IP2:port2)
If login data does not go through the device, please set listening mirror port (which should be idle)
LAN
DMZ
WAN1
WAN2
WAN3
Users belonging to following network segment must use SSO (but users that require Dkey or no authentication are excepted)
Format: One IP range or subnet per row
IP range: start IP-end IP, e.g. 192.168.0.1-192.168.0.6
Subnet: IP/mask, e.g. 192.168.0.1/255.255.255.0
192.168.30.117
Page Display After Authentication
Authentication Conflict Settings
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)
Other Authentication Options
OK

7.2.2.1. Active Directory SSO

When the host of the user logs in to the active directory server (not for the first time), it will automatically passing the WEB authentication, without typing the username and password once again.

Typical topology of Active Directive SSO is as shown below:



The domain controller locates in the local area network, that is to say, PC1 and PC2 can log in to the domain controller before authentication; the domain controller and IAM gateway device can communicate with each other, so that the domain controller can send the successfully-authenticated user information to the IAM gateway device. The primary DNS of the LAN user (PC) should be the same with the IP address of the domain controller.

Check [Enable Active Directory SSO] to activate this SSO function. Click <Help of SSO Usage> to view the guide information of how to configure component mode of SSO.

Active Directory SSO falls into three types: one is to install a SSO script on the domain controller to intercept the logon logs; the second one is to allocate SSO script by the domain controller; the third one is to allocate SSO script by the domain controller and to send logon/logoff information to the IAM gateway device. The last SSO should have the help of a listening port to intercept the active directory SSO information (in the data) sent from the mirror port of the switch or from the HUB.

7.2.2.1.1. Install Component Mode

Enter the shared key in the text box followed [User component mode, please enter shared key], ensuring that the key is the same with that configured in the SSO component of the domain controller.

At the end of installing the SSO component of the domain controller, it requires typing IP address of the IAM gateway device, shared key. The shared key must be the same with that configured on the IAM gateway device; otherwise, the active directory SSO function will not work properly.

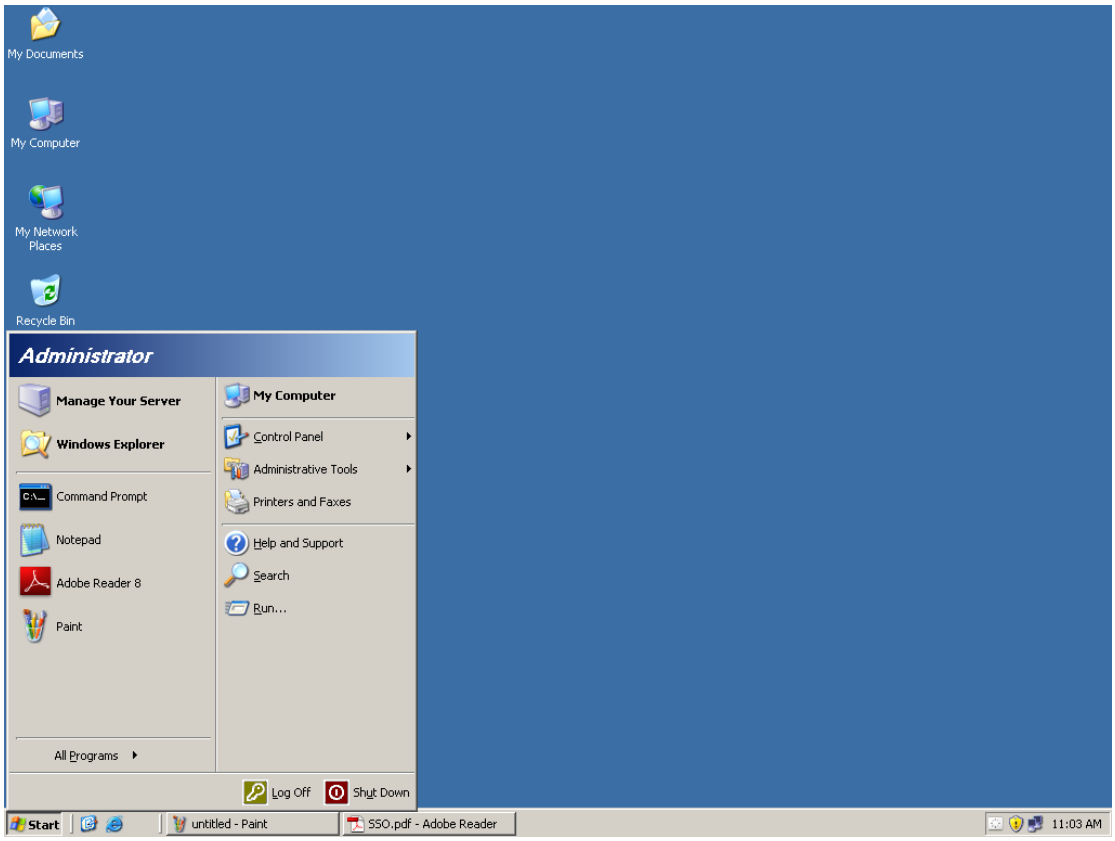
7.2.2.1.2. AD Group Policy Mode

This mode can realize SSO with the help of group policy of the Active Directory. Configured correctly, it will enable the user to automatically get WEB authentication fulfilled by the IAM

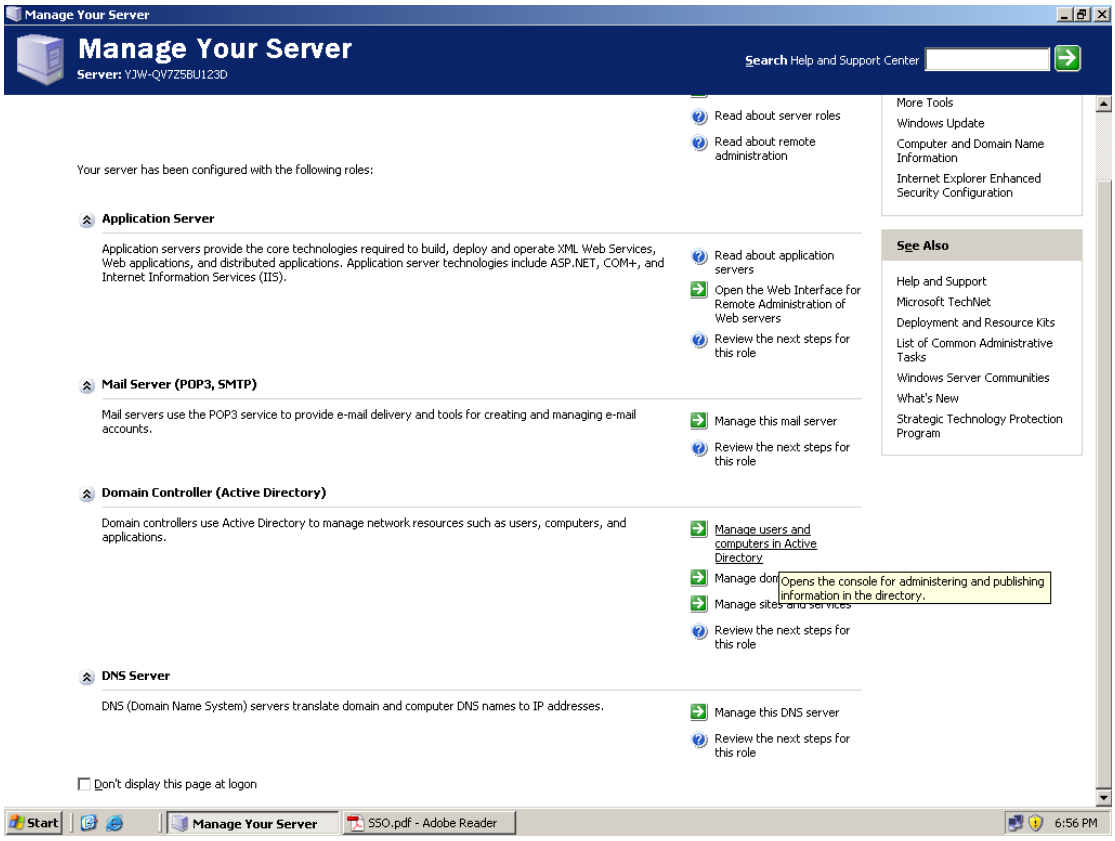
gateway device when the user logs in to the Active Directory, and will enable the user to logoff from the IAM gateway device when it is logging off.

7.2.2.1.3. Configure Logon Script Program

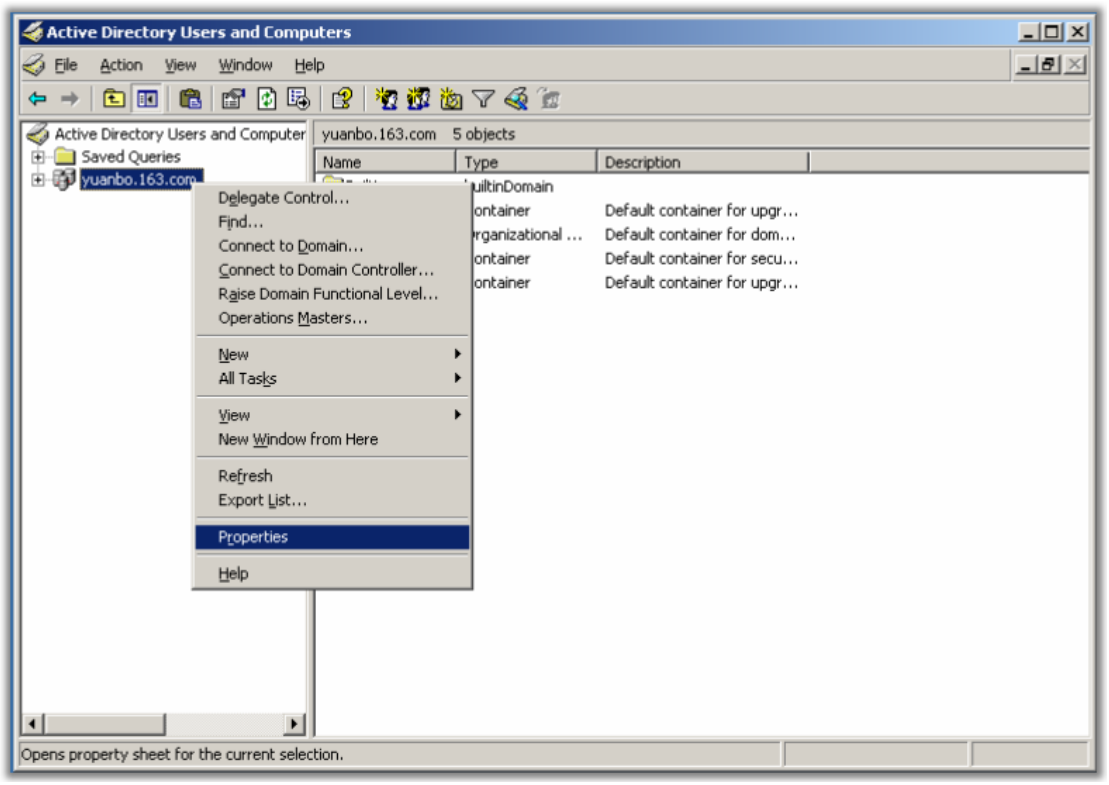
Logging in to the domain controller, click [Start] > [Program] > [Administrator Tool] > [Manage Your Server], as shown below:



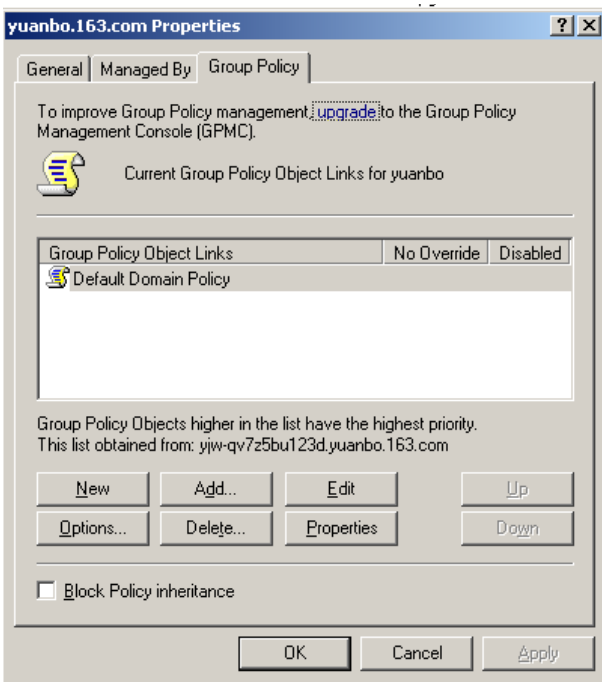
Select [Manage users and computers in Active Directory], as shown below:


Manage Your Server
Manage Your Server
Server: YJW-QV7Z5BU123D
Search Help and Support Center
Read about server roles
Read about remote administration
More Tools
Windows Update
Computer and Domain Name Information
Internet Explorer Enhanced Security Configuration
Your server has been configured with the following roles:
Application Server
Application servers provide the core technologies required to build, deploy and operate XML Web Services, Web applications, and distributed applications. Application server technologies include ASP.NET, COM+, and Internet Information Services (IIS).
Read about application servers
Open the Web Interface for Remote Administration of Web servers
Review the next steps for this role
See Also
Help and Support
Microsoft TechNet
Deployment and Resource Kits
List of Common Administrative Tasks
Windows Server Communities
What's New
Strategic Technology Protection Program
Mail Server (POP3, SMTP)
Mail servers use the POP3 service to provide e-mail delivery and tools for creating and managing e-mail accounts.
Manage this mail server
Review the next steps for this role
Domain Controller (Active Directory)
Domain controllers use Active Directory to manage network resources such as users, computers, and applications.
Manage users and computers in Active Directory
Opens the console for administering and publishing information in the directory.
Review the next steps for this role
DNS Server
DNS (Domain Name System) servers translate domain and computer DNS names to IP addresses.
Manage this DNS server
Review the next steps for this role
Don't display this page at logon
Start
Manage Your Server
SSO.pdf - Adobe Reader
6:56 PM

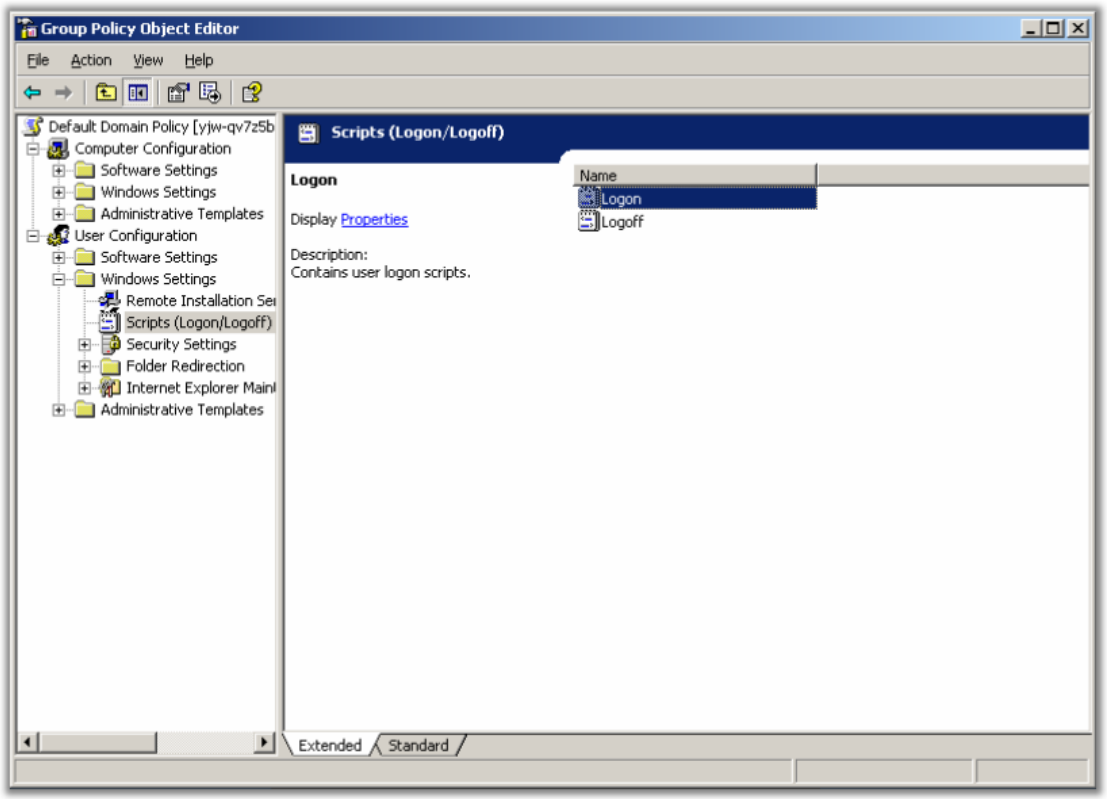
Right click the to-be-monitored directory in the pop-up window, and click [Properties], as shown below:



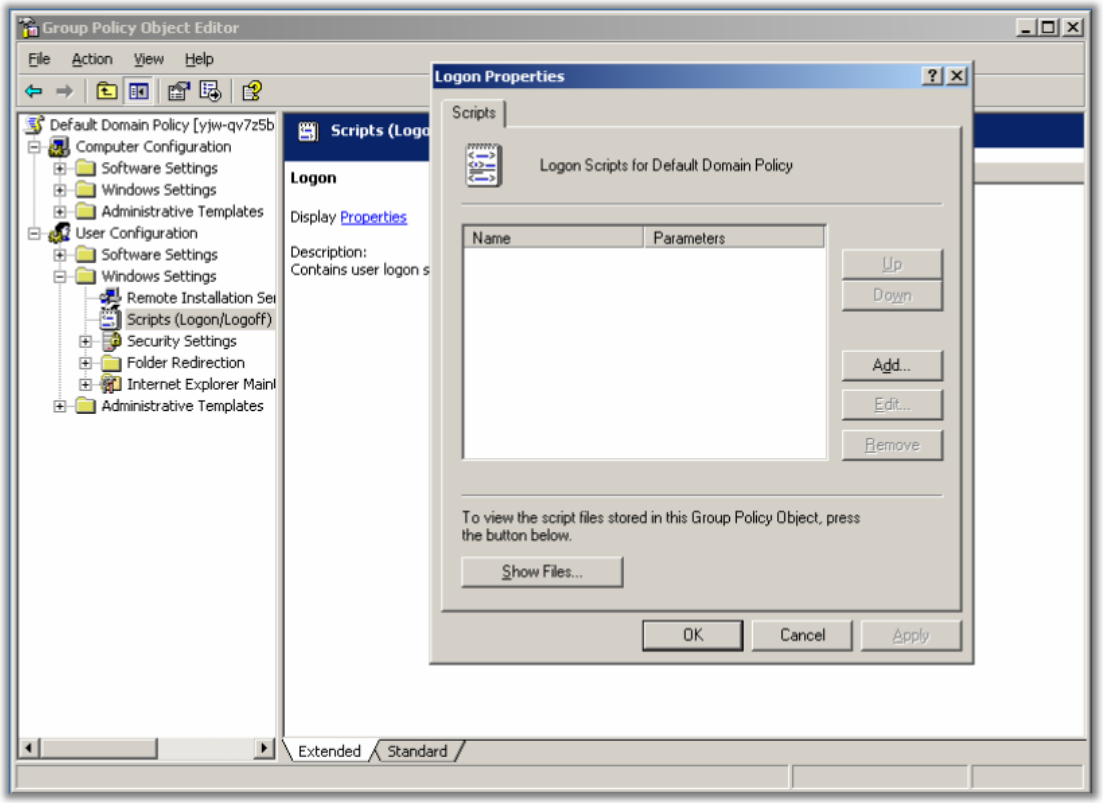
Select [Group Policy] and then [Default Domain Policy], as shown below:



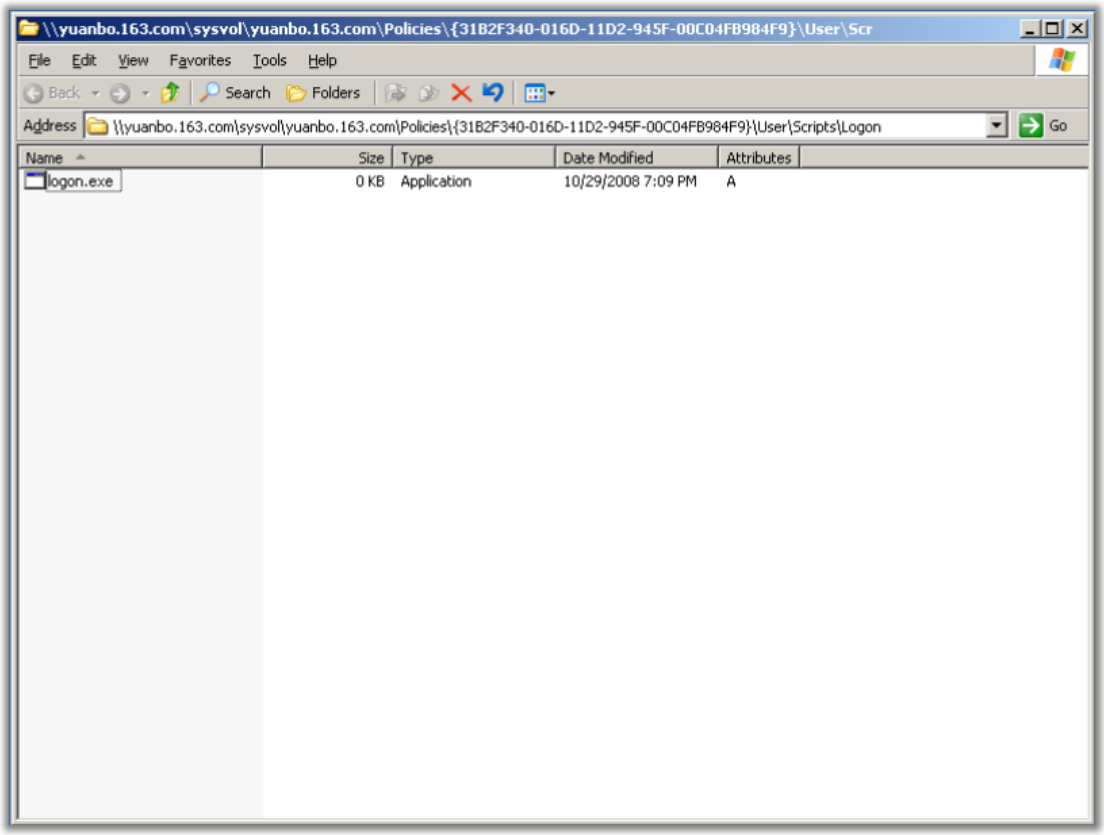
Then click [User Configuration] > [Windows Settings] > [Scripts (Logon/Logoff)] in the pop-up [Group Policy Object Editor], as shown below:



Double click [Logon] item, and the [Logon Properties] dialog appears, as shown below:

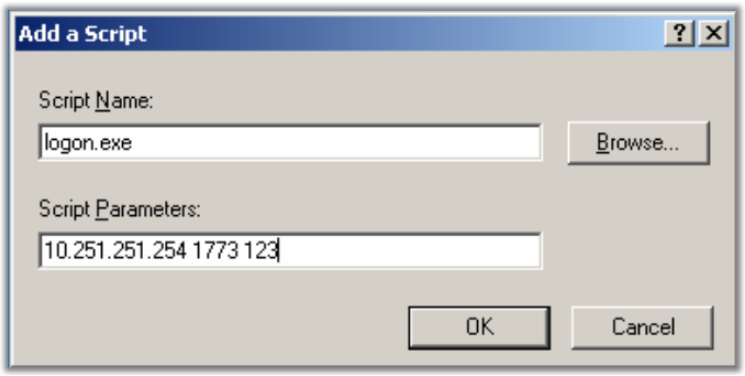


Click the <Show Files> button, and a directory is opened. Save the *logon.exe* script file into this director and close the window.



Under the [Logon Properties] dialog, click the <Add> button to enter the [Add a Script] dialog. Click <Browse> to upload the *logon.exe* script file and enter [Script Parameters] the IP address (IP address of the IAM gateway device), the port number (1773) and shared key (must be the same with that configured on the IAM gateway device). Parameters are separated from each other by a blank space.

Then click the <Apply> and the <OK> buttons; close all the [Group Policy Object Editor], etc.

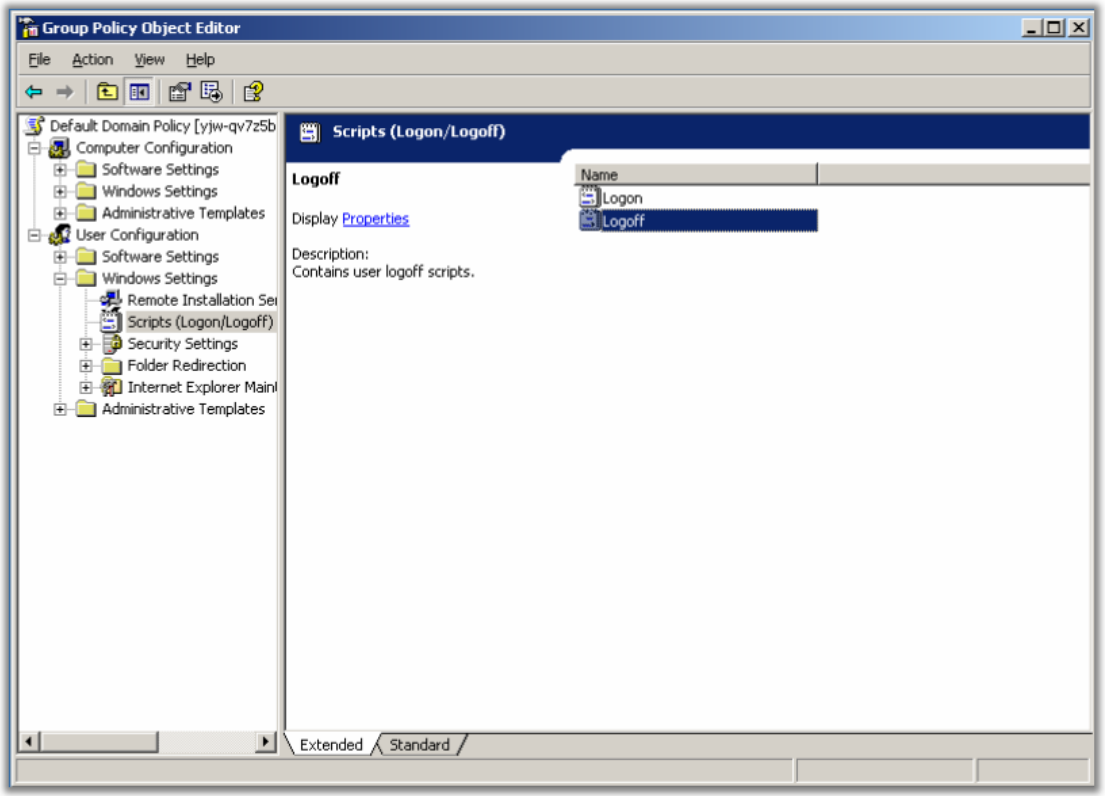


Having completed configuring the logon script, you have to click [Start] > [Run] and type the "**gpupdate**" and click the <OK> button to have the group policy configurations take effect.

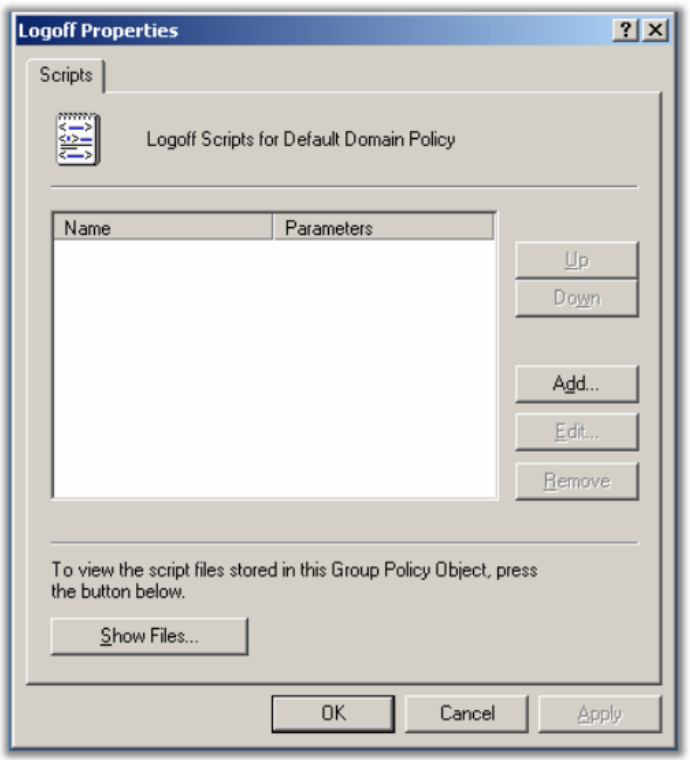
Till then, the logon script program is added successfully. When the directory user logs in, this logon script program will run.

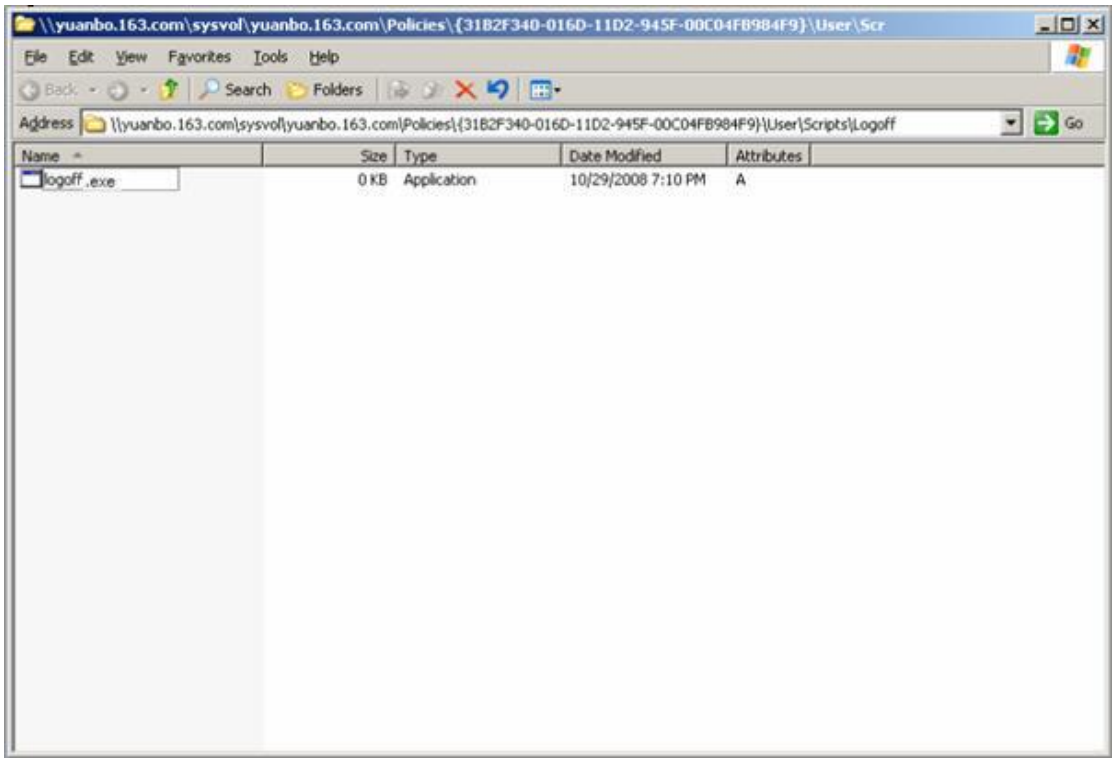
7.2.2.1.4. Configure Logoff Script Program

Follow the steps (same with that in [Configure Logon Scrip Program]. Please refer to the above section) and enter the [Group Policy Object Editor] page; click [User Configuration] > [Windows Settings] > [Scripts (Logon/Logoff)], and then double click the [Logoff] item, as shown below:

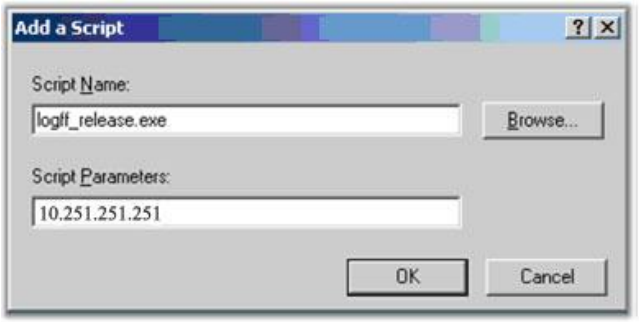


Under the pop-up [Logoff Properties] dialog, click the <Show Files> button to open a directory and save the logoff script (that is, the *logoff.exe* file). And then close the directory.





Click the <Add> button in the pop-up [Logoff Properties] dialog, and the [Add a Script] dialog appears (as shown below). Click the <Browse> button to upload the logoff script file (that is the *logoff.exe* file) and enter the [Script Parameters] (the IP address 10.251.251.251). Then close the related configuration dialog/page one by one.



Having completed configuring the logoff script, you have to click [Start] > [Run] and type the "**gpupdate**" and then click the <OK> button to have the group policy take effect.

Till then, the logoff script grogram is configured successfully. When the directory user logs off, this logoff script program will run.

- The primary DNS of the user host must be the IP address of the domain controller, otherwise,

the domain controller will not be found when the user is added to the domain.

- If a user has logged in to the Active Directory successfully but the primary DNS or IP address is modified later, single sign-on (SSO) will get invalid; though, it seems that the user can still use the correct password to successfully log in. In fact, it only indicates that the user is getting into the Windows instead of the domain, for user will be still required for password to log in to the domain. This is because that Windows can remember the previous correct login password and allows the user to enter Windows, but actually it is not a successful logon to the domain controller.
- Domain server IP address, LAN IP address of the IAM gateway device and the user's computer should be able to communicate with each other. This OSS functions only when the LDAP authentication is enabled, and that the user logs in to the domain controller through its computer.
- To use monitoring mode, check [Use monitoring mode] and type the IP address and port of the domain controller in the [Login server] text box. This configuration can help to listen to the information that the client gets authenticated to the domain controller.
- If the authentication does not have the IAM gateway device get involved, listening mode SSO is available only when the listening port is configured. As to the detailed configuration of a listening port, please refer to Section 7.2.2.5 SNMP Option.
- It is better to enable several SSO modes at the same time.

7.2.2.2. POP3 SSO

7.2.2.2.1. POP3 Authentication

POP3 authentication is generally applicable to internal mail system, and each user has been allocated with an email account. It is flexible for the client's email environment and improves the variety of authentication methods, and makes the authentication process more convenient and humane.

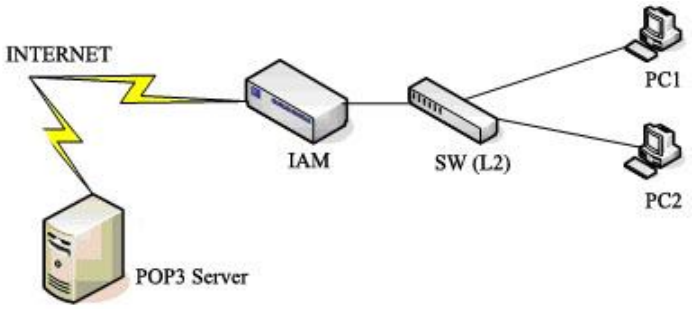
As to configuring POP3 authentication, the user should be an existing user of POP3 server. If the

user enters username, password and the authentication system can successfully log in to the assigned POP3 server, the password entered by the user is then proved correct, and the user will get authenticated; if it fails to log in, then the user cannot get authenticated.

Check the [Enable POP3 SSO] option, and the authentication system will automatically identify the authentication information and allow the authenticated user to get access to the Internet directly when the user is logging into the POP3 server through mail client such as Outlook, Foxmail, etc., without requiring it to type once again the username and password.

7.2.2.2.2. Network Environment

Typical topology (environment) of the POP3 authentication is as shown in the following figure:



If both the POP3 server and PC are in the local area network, the authentication data will not be forwarded to the IAM gateway device. Automatic authentication is realized through the mirror port; if there is no mirror port, the user has to manually get authenticated, that is to say, the user has to type the username and password when browsing a webpage.

7.2.2.2.3. Configuration

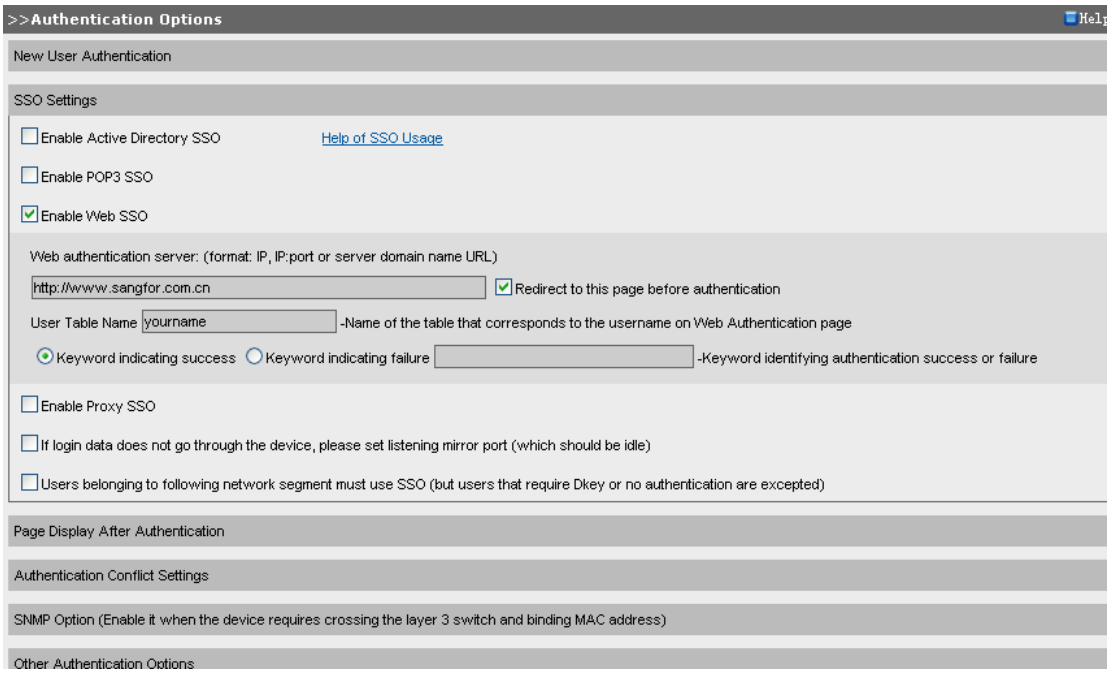
Check [Enable POP3 SSO], and type the IP address and port in the [Login server] text box, which will enable the IAM gateway device to listen to the authentication information that the client host gets authenticated through the POP3 server.

- If the authentication does not have the IAM gateway device get involved, SSO is available only when a listening port is configured first. As to the configuration of a listening port, please refer to Section 7.2.2.5 SNMP Option.

- If the POP3 server is in the external network, to achieve SSO, you have to check the option [Allow users to access DNS service before authentication] (in [IAM] > [Authentication Options] page> [Other Authentication Options]), and entitle the user's root group the privilege to access the POP3 server.

7.2.2.3. WEB SSO

[Enable Web SSO]: Check this option to enable the Web single sign-on function.


>>Authentication Options
New User Authentication
SSO Settings
Enable Active Directory SSO
Help of SSO Usage
Enable POP3 SSO
Enable Web SSO
Web authentication server: (format: IP, IP:port or server domain name URL)
http://www.sangfor.com.cn
Redirect to this page before authentication
User Table Name yourname
-Name of the table that corresponds to the username on Web Authentication page
Keyword indicating success
Keyword indicating failure
-Keyword identifying authentication success or failure
Enable Proxy SSO
If login data does not go through the device, please set listening mirror port (which should be idle)
Users belonging to following network segment must use SSO (but users that require Dkey or no authentication are excepted)
Page Display After Authentication
Authentication Conflict Settings
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)
Other Authentication Options

[Web authentication server: (format: IP or IP: port, or server domain name URL)]: Type the server in the text box for Web SSO, as shown below:

>>Authentication Options
Help
New User Authentication
SSO Settings
Enable Active Directory SSO
Help of SSO Usage
Enable POP3 SSO
Enable Web SSO
Web authentication server: (format: IP, IP:port or server domain name URL)
200.200.200.1:80
Redirect to this page before authentication
User Table Name pwduser
-Name of the table that corresponds to the username on Web Authentication page
Keyword indicating success
Keyword indicating failure
get pass
-Keyword identifying authentication success or failure
Enable Proxy SSO
If login data does not go through the device, please set listening mirror port (which should be idle)
Users belonging to following network segment must use SSO (but users that require Dkey or no authentication are excepted)
Page Display After Authentication
Authentication Conflict Settings
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)
Enable
Disable

[Redirect to this page before authentication]: Check this option, and the webpage being browsed will be redirected to the configured page for Web SSO if the user has not been authenticated yet.

[User Table Name]: Configures the name of the user table to be handed in to the server when user is getting Web authentication.

[Keyword indicating success], [Keyword indicating failure]: Configures the keyword according to which the Web SSO authentication of the user is identified as a success or a failure. If you have checked [Keyword indicating success] and the keyword is contained in the return results of POST, the authentication would be regarded as a success. If you have checked [Keyword indicating failure] and the keyword is contained in the return results of POST, the authentication would be regarded as a failure.

- Length of the keyword and table for Web authentication must be less than 96 bytes and cannot be 0.
- If the authentication does not have the IAM gateway device get involved, SSO is available only when a listening port is configured first. As to the configuration of a listening port, please refer to Section 7.2.2.5.

7.2.2.4. Proxy SSO

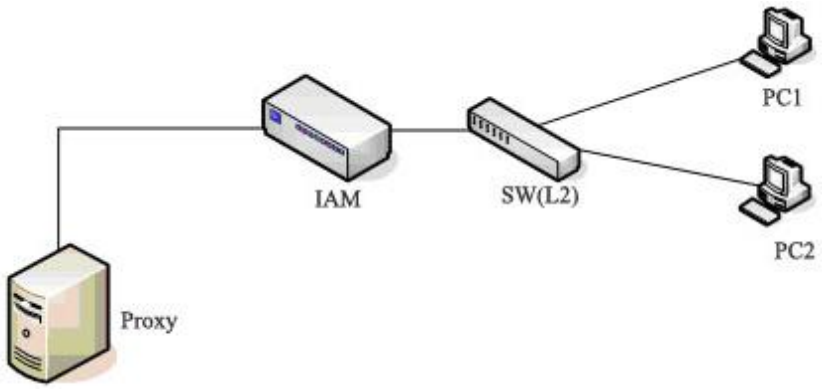
7.2.2.4.1. Proxy Authentication

Proxy authentication is generally applicable to the environment that the users get access to the Internet through Proxy, and that each user has been allocated with a proxy account.

It is flexible for the client's proxy environment. While configuring Proxy authentication, the user should be an existing user of the Proxy server. If the user wants to access the Internet through Proxy server, it must enter the correct username and password to get authenticated; if verification fails, authentication will fail as well. The IAM gateway device will then associate the IP address and the user according to the intercepted information of Proxy authentication.

7.2.2.4.2. Network Environment

Typical topology (environment) of Proxy authentication is as shown in the following figure:



If the IAM gateway device is under Bypass mode, the authentication data will not be forwarded to the IAM gateway device. Automatic authentication is realized through the mirror port; if there is no mirror port, the user has to manually get authenticated, that is to say, the user has type the username and password when browsing a webpage.

7.2.2.4.3. Configuration

Check [Enable Proxy SSO], and type the IP address and port in the [Login server] text box, which will enable the IAM gateway device to listen to the authentication information that the client host gets authenticated through the Proxy server.

If the authentication does not have the IAM gateway device get involved, SSO is available only when a listening port is configured first. As to the configuration of a listening port, please refer to Section 7.2.2.5 SNMP Option.

7.2.2.5. Listening Mirror Port

Listening mirror port functions when the authentication does not have the IAM gateway device get involved. The interface (mirror port of the switch) listens to the authentication information intercepted over the network, which helps to achieve single sign-on.

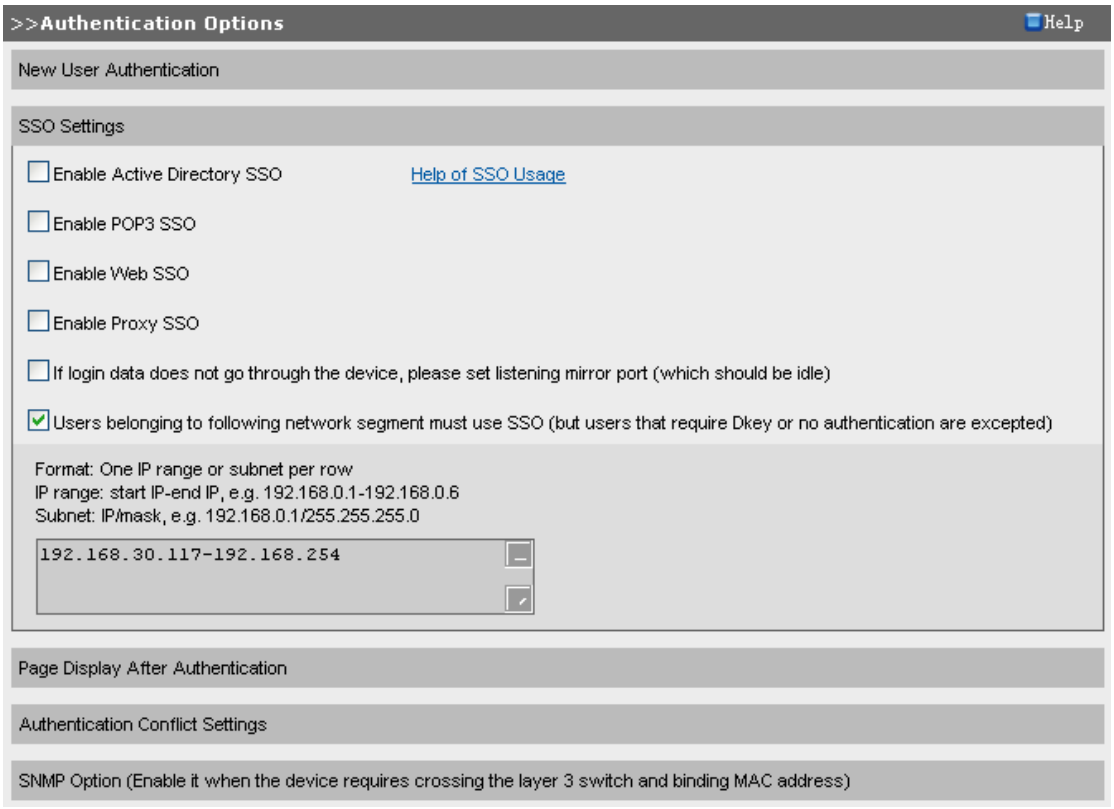
Check [If login data does not go through the device, please set listening mirror port (which should be idle)] and select an idle network interface that will act as the listening port.

- The listening port must be a port that is not being used by the IAM gateway device.
- The mirror port (of the switch) must mirror at least the network interface of the authentication server.

7.2.2.6. Only Allow SSO

[Users belonging to following network segment must use SSO (but users that require DKEY or no authentication are excepted)]: Configures the IP ranges of some LAN user(s) who can only (must) log in with SSO.

The configuration page is as shown below:

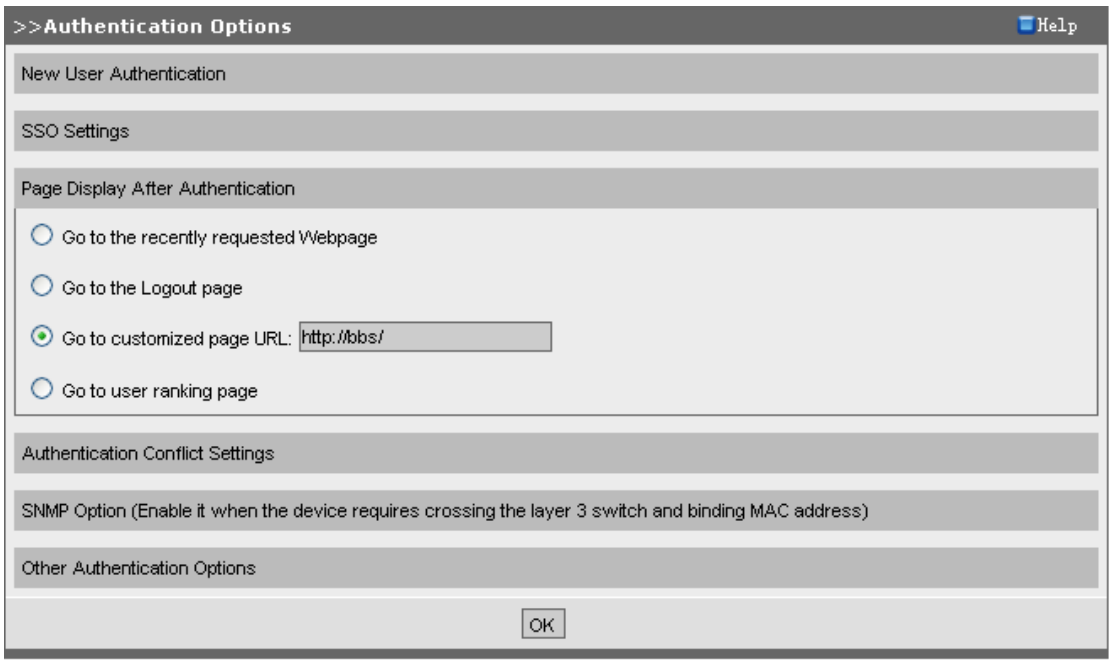

>>Authentication Options
Help
New User Authentication
SSO Settings
Enable Active Directory SSO
Help of SSO Usage
Enable POP3 SSO
Enable Web SSO
Enable Proxy SSO
If login data does not go through the device, please set listening mirror port (which should be idle)
Users belonging to following network segment must use SSO (but users that require Dkey or no authentication are excepted)
Format: One IP range or subnet per row
IP range: start IP-end IP, e.g. 192.168.0.1-192.168.0.6
Subnet: IP/mask, e.g. 192.168.0.1/255.255.255.0
192.168.30.117-192.168.254
Page Display After Authentication
Authentication Conflict Settings
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)

Type single IP address(es) or IP range(s) in the text box. The IP address(es) contained in this list has to get SSO authentication through the IAM gateway device, otherwise, it cannot access the Internet. It is an exception if some users have bound any of the IP address in this list but have checked [None] for [Authentication Method] (please refer to [IAM] > [Organization Structure] > [Edit User] page > [Advanced Settings] > [User Attribute], or Section 7.4.5 Edit User), or some users have enabled [DKEY] for [Authentication Method], that is to say, these users need not use SSO to access the Internet.

7.2.3. Page Display After Authentication

[Page Display After Authentication] configured for the redirected-to page after the user passes the WEB authentication.

The configuration page is as shown below:


>>Authentication Options
Help
New User Authentication
SSO Settings
Page Display After Authentication
Go to the recently requested Webpage
Go to the Logout page
Go to customized page URL:
http://bbs/
Go to user ranking page
Authentication Conflict Settings
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)
Other Authentication Options
OK

[Go to the recently requested Webpage]: If the user gets authenticated successfully, the WEB page will be redirected to the page that is requested by the user before successful authentication.

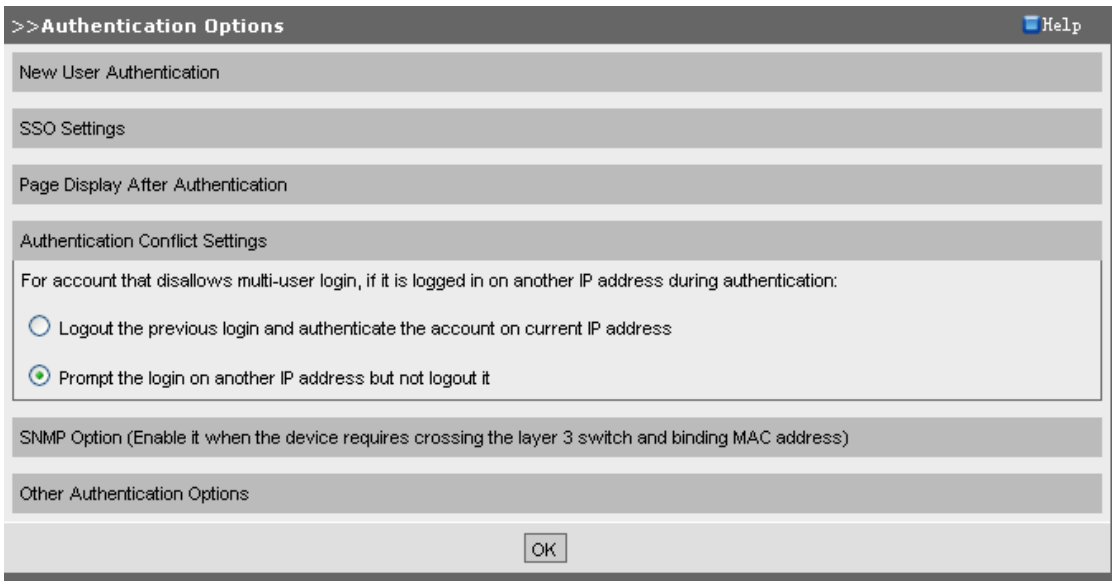
[Go to the Logout page]: If the user gets authenticated successfully, the Web page will be redirected to the logout page.

[Go to customized page URL]: If the LAN user gets authenticated successfully, the Web page will be redirected to the user-defined page.

[Go to user ranking page]: If the LAN user gets authenticated successfully, the Web page will be redirected to a ranking statistics page (of the internal Data Center).

7.2.4. Authentication Conflict Settings

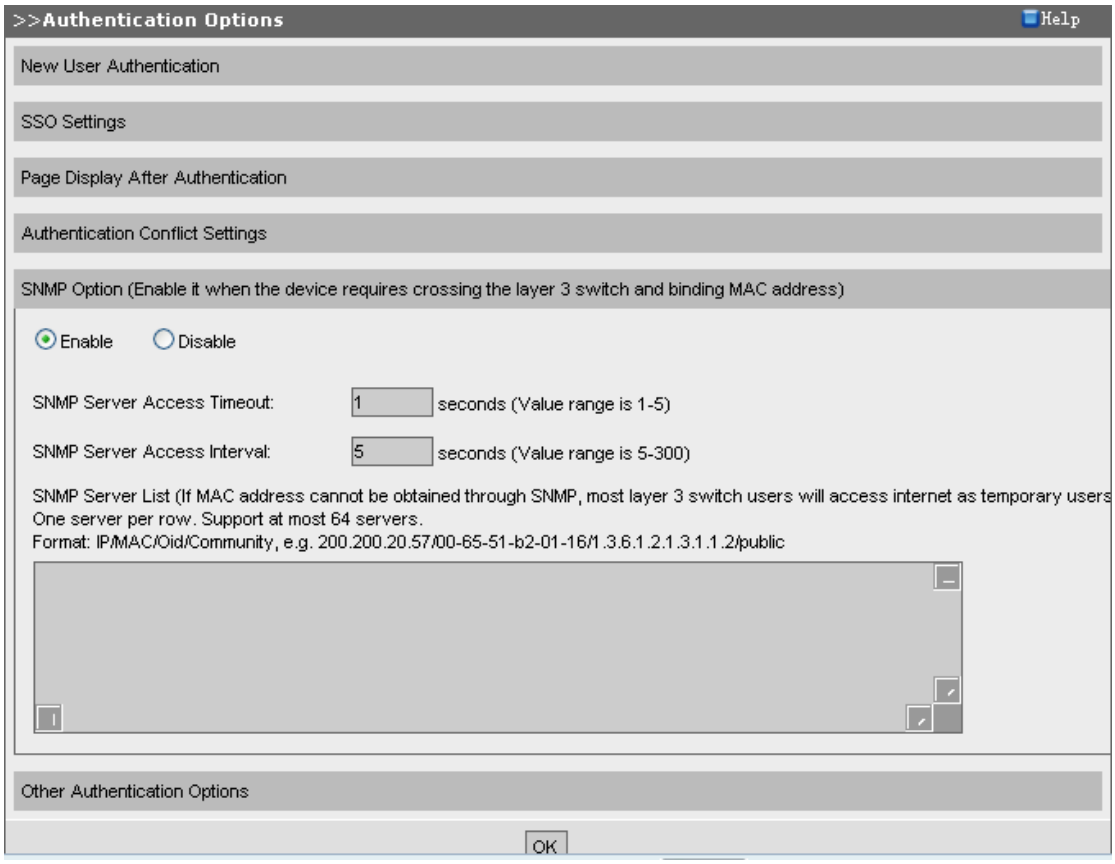
[Authentication Conflict Settings] defines the handling method of the IAM gateway device, if it is found that there are several users logging in with a same account but this account does not allow multiple users to log in with it. Options are [Logout the previous login and authenticate the account on current IP address] and [Prompt the login on another IP address but not logout it].


>>Authentication Options
Help
New User Authentication
SSO Settings
Page Display After Authentication
Authentication Conflict Settings
For account that disallows multi-user login, if it is logged in on another IP address during authentication:
Logout the previous login and authenticate the account on current IP address
Prompt the login on another IP address but not logout it
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)
Other Authentication Options
OK

7.2.5. SNMP Option

[SNMP Option] helps to achieve Internet access through binding MAC, or binding IP and MAC address when a layer 3 switch exists in the networking environment.

The configuration page is as shown below:


>>Authentication Options
Help
New User Authentication
SSO Settings
Page Display After Authentication
Authentication Conflict Settings
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)
Enable
Disable
SNMP Server Access Timeout:
1
seconds (Value range is 1-5)
SNMP Server Access Interval:
5
seconds (Value range is 5-300)
SNMP Server List (If MAC address cannot be obtained through SNMP, most layer 3 switch users will access internet as temporary users
One server per row. Support at most 64 servers.
Format: IP/MAC/Oid/Community, e.g. 200.200.20.57/00-65-51-b2-01-16/1.3.6.1.2.1.3.1.1.2/public
Other Authentication Options
OK

[Enable], [Disable]: Select it to enable or disable the [SNMP Option] function.

[SNMP Server Access Timeout], [SNMP Server Access Interval]: Configures the timeout and the time interval that the layer 3 switch is accessed. The default value is recommended.

[SNMP Server List]: Type the IP address, MAC address, SNMP Oid and the community of the layer 3 switch in the text box. Different elements are separated from each other with a back slash (/), for instance, 192.168.30.245/00-0f-e2-59-0c-1f/1.3.6.1.2.1.3.1.1.2/public.

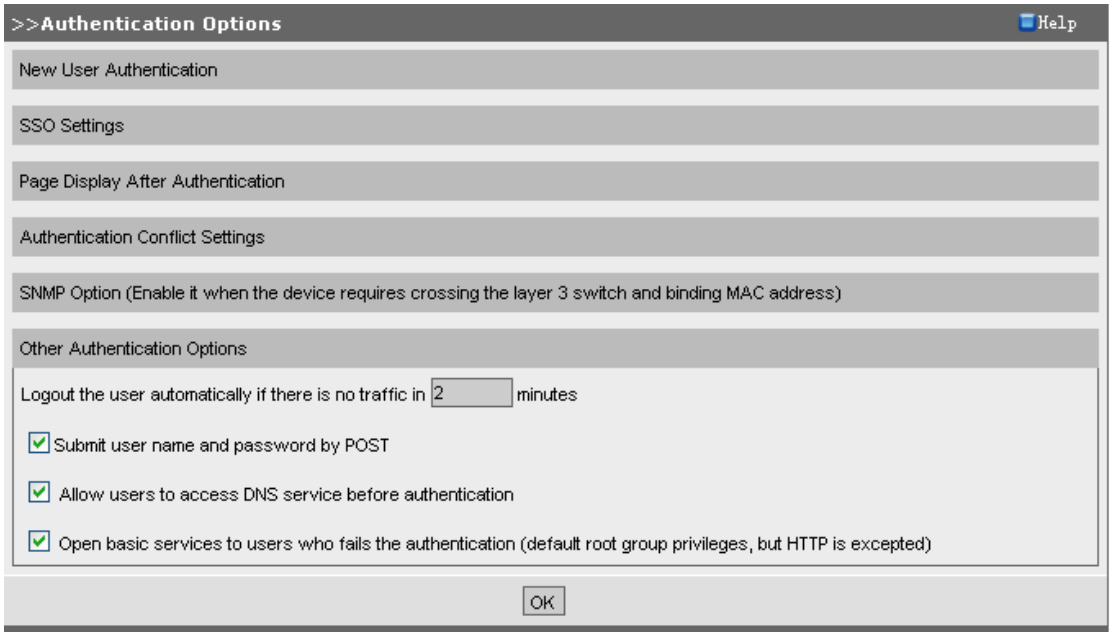
Having completed configuring the page, you have to click the <OK> button to save the settings.

If you enable and configure [SNMP Option], the layer 3 switch must support SNMP services, and the community of the layer 3 switch and the SNMP version must be configured correctly.

7.2.6. Other Authentication Options

[Other Authentication Options] configures the other authentication-related options, including automatic logout time, DNS service availability for users who fail to get authenticated.

The configuration page is as shown below:


>>Authentication Options
Help
New User Authentication
SSO Settings
Page Display After Authentication
Authentication Conflict Settings
SNMP Option (Enable it when the device requires crossing the layer 3 switch and binding MAC address)
Other Authentication Options
Logout the user automatically if there is no traffic in 2 minutes
Submit user name and password by POST
Allow users to access DNS service before authentication
Open basic services to users who fails the authentication (default root group privileges, but HTTP is excepted)
OK

[Logout the user automatically if there is no traffic in _ minutes]: If there is no traffic caused by

this user in certain time (it is 120 minutes by default), this user will automatically log out.

[Submit user name and password by POST]: Check this option, and the user will get authenticated through Web, with the correct username and password.

[Allow users to access DNS service before authentication]: Check this option, and the user is allowed to access DNS before successful authentication.

[Open basic services to users who fail to authentication (default root group privileges, but HTTP is excepted)]: Check this option, and the privileges of root group on various service and applications (HTTP service excluded) are also available for the users who have not yet gotten authenticated.

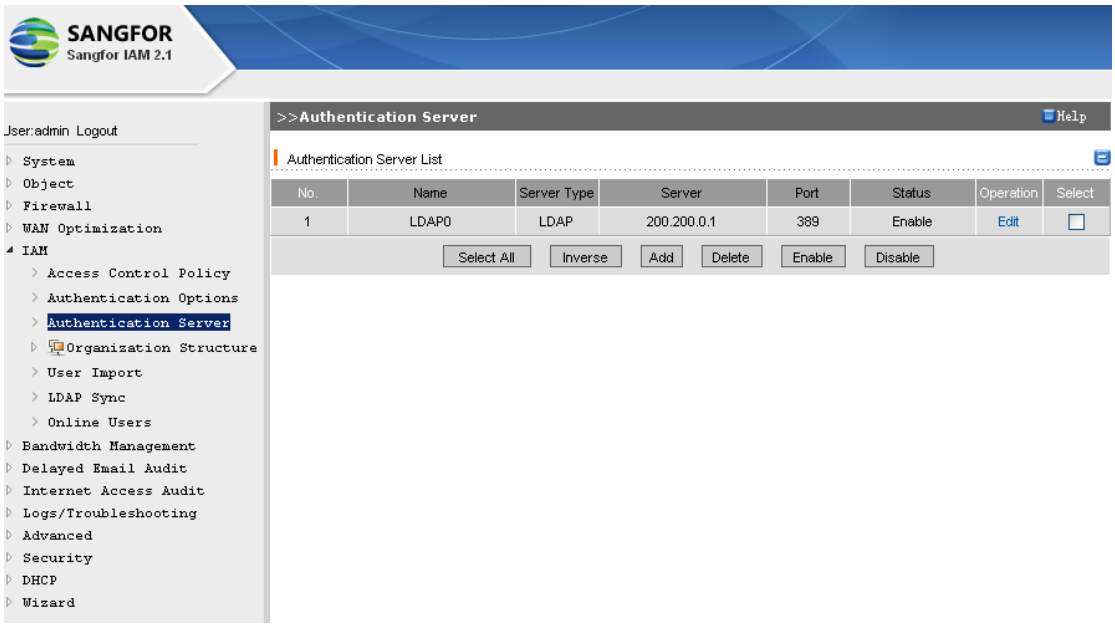
- With [Password] as the [Authentication Method], the user can modify its own password, without the help of the administrator. However, if incorrect password is entered more than three times (consecutive inputs), this user will be blocked for one minute.
- To modify the password, procedures are: type http://0.0.0.0 (IP address of the IAM gateway device) to open the [Identity Authentication System] page, and then click the link <Modify Password> to enter the [Modify Password] page to replace the old password with a new one, as shown below:

- If [DKEY] is the [Authentication Method], the user has to click the <DKEY Client> link to download the [DKEY Client], as shown in the two figures above.
- Also, if the Ingress Client fails to be installed automatically, the user can also click the link <Ingress Client> to download and manually install the Ingress Client.

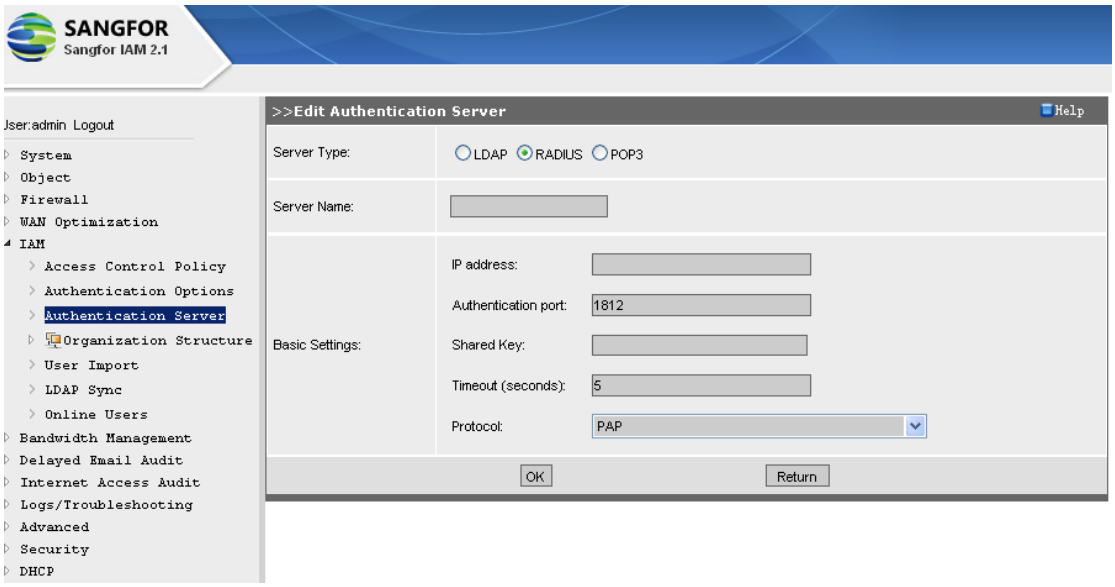
7.3. Authentication Server

[Authentication Server]: Configures the third-party authentication server. SANGFOR IAM gateway device supports three authentication servers in the external networks, namely, LDAP, RADIUS and POP3.

The default configuration page of [Authentication Server] is as shown below:



Click the <Add> button, and the [Edit Authentication Server] page appears, as shown below:

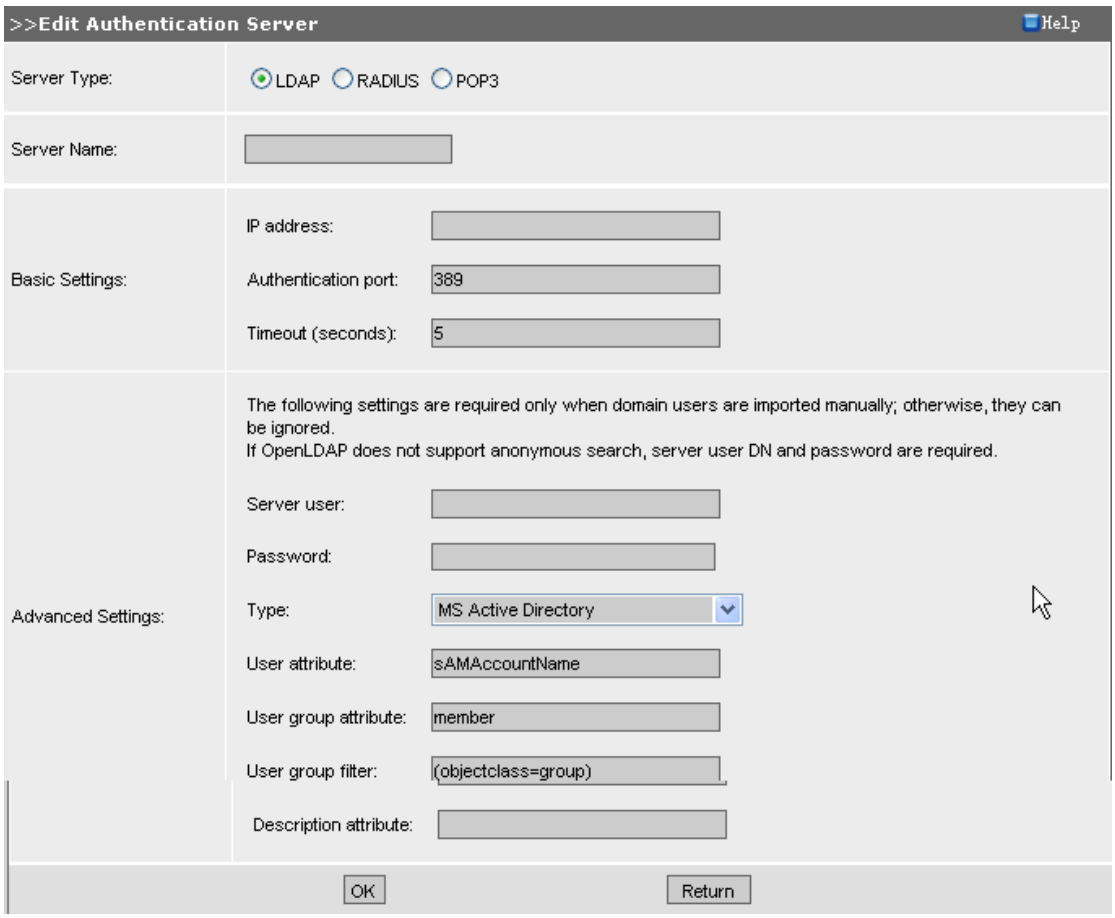


[Server Type]: Select the needed server to open the corresponding settings.

7.3.1. LDAP

[LDAP] server supports Microsoft SGtive Directory, SUN LDAP and OPEN LDAP server. You can select a needed one according to your case.

The configuration page of [LDAP] is as shown below:

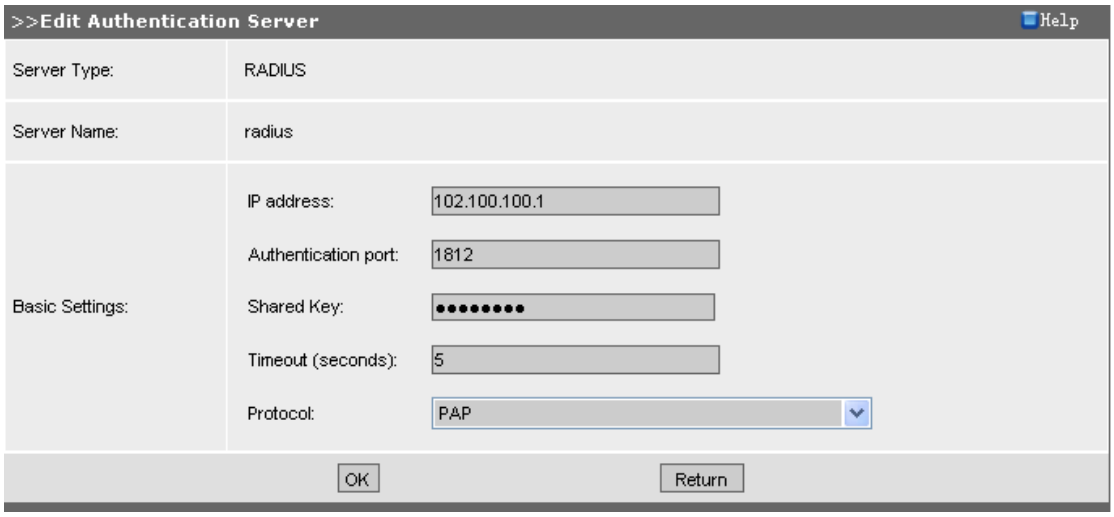


Generally, you need only configure [IP address], [Authentication port], [Server User], [Password] and [Types]; other settings are recommended to be the defaults. If necessary, please turn to the system administrator of LDAP server for detailed configuration guide to this page.

- [Server Name] can only contain English characters. Otherwise, you may fail to import the AD users and fail to read the AD structure.
- Generally, [Server User] is the admin account, in format of Administrator@domain.com.

7.3.2. RADIUS

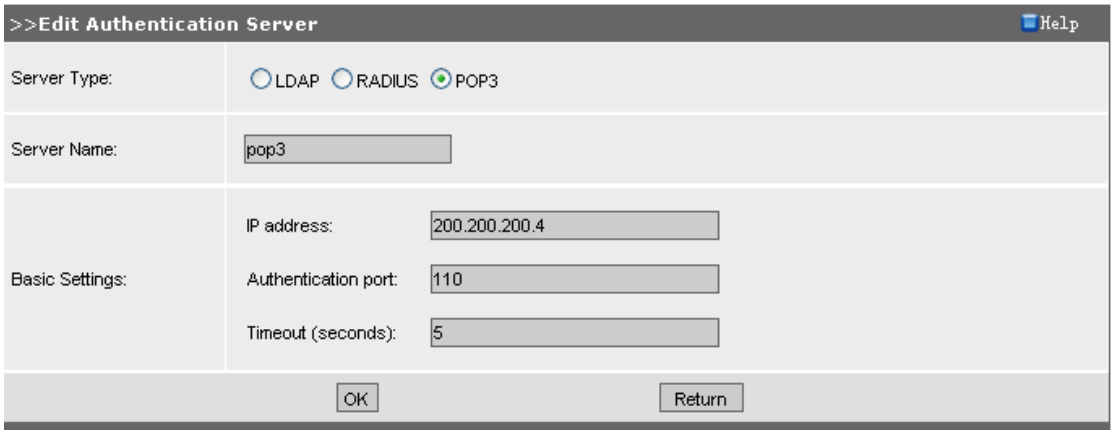
The [RADIUS] server configuration page is as shown below:



Generally, you need only configure [IP address], [Authentication port], [Shared key], [Timeout] and [Protocol]. If necessary, please turn to the system administrator of RADIUS server for detailed configuration guide to this page.

7.3.3. POP3

[POP3] server configuration page is as shown below:

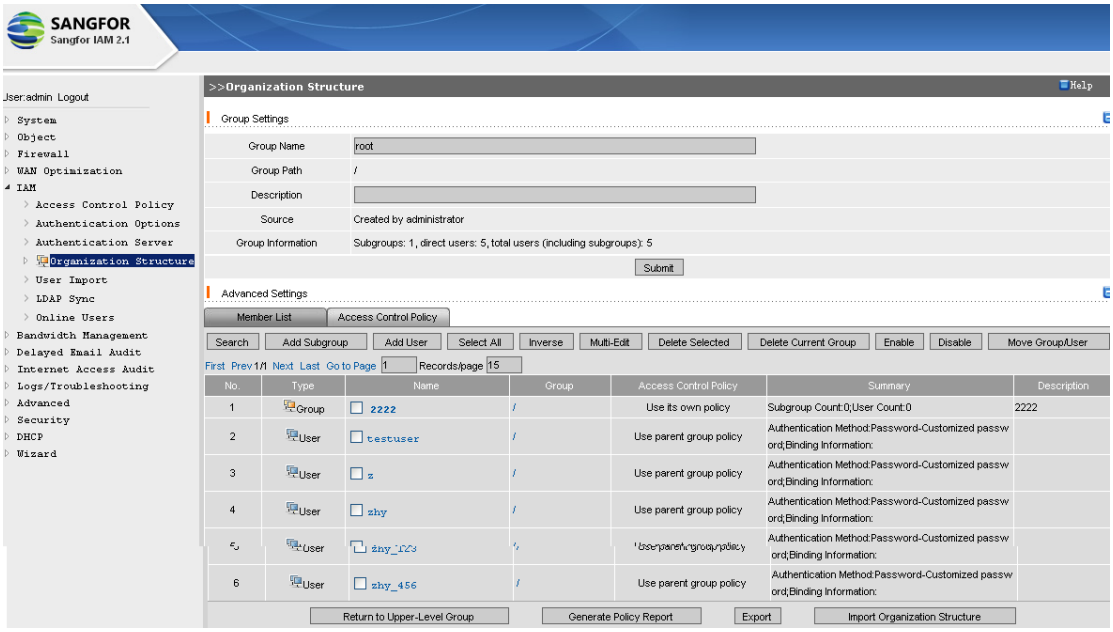


You can configure the [IP address], [Authentication port] and [Timeout] for the POP3 server.

7.4. Organization Structure

[Organization Structure]: Configured the structure of the LAN users and user groups, as well as the association between the policy and user group.

The default [Organization Structure] configuration page is as shown below:



As shown above, there is a built-in group, root group of the [Member List]. The root group cannot be deleted, and its name cannot be modified. The user-defined groups are subgroups of the root group.

You can configure the relationship between the groups, inheriting the properties of a group or belonging to a group, which helps you to distinguish parent group(s) from subgroup(s) and parent group(s) from user(s). The structure and relations listed are similar to the structure of and relations in an enterprise.

[Member List]: Displays the subgroup(s) and user(s) of the current root group or subgroup.

[Access Control Policy]: Displays the associated access control policy (policies) of the current root group, subgroup or user.

[No.]: Sequence number of this member in the current group.

[Type]: Type of the member, group (subgroup) or user.

[Name]: Name of each member.

[Group]: The path (group) that the member locates in.

[Access Control Policy]: Lists the type of the access control policy or policies associated with the member, [Use parent group policy] or [Use parent group policy]. [Use its own policy] indicates that the associated access control policy (policies) is exactly the same with that (those) of its parent group, inhering from its parent group, and itself cannot add, delete or edit policy. [Use it own policy] indicates that the member can have its own access control policy instead of inhering only from its parent group.

[Summary]: Displays the brief information of each member.

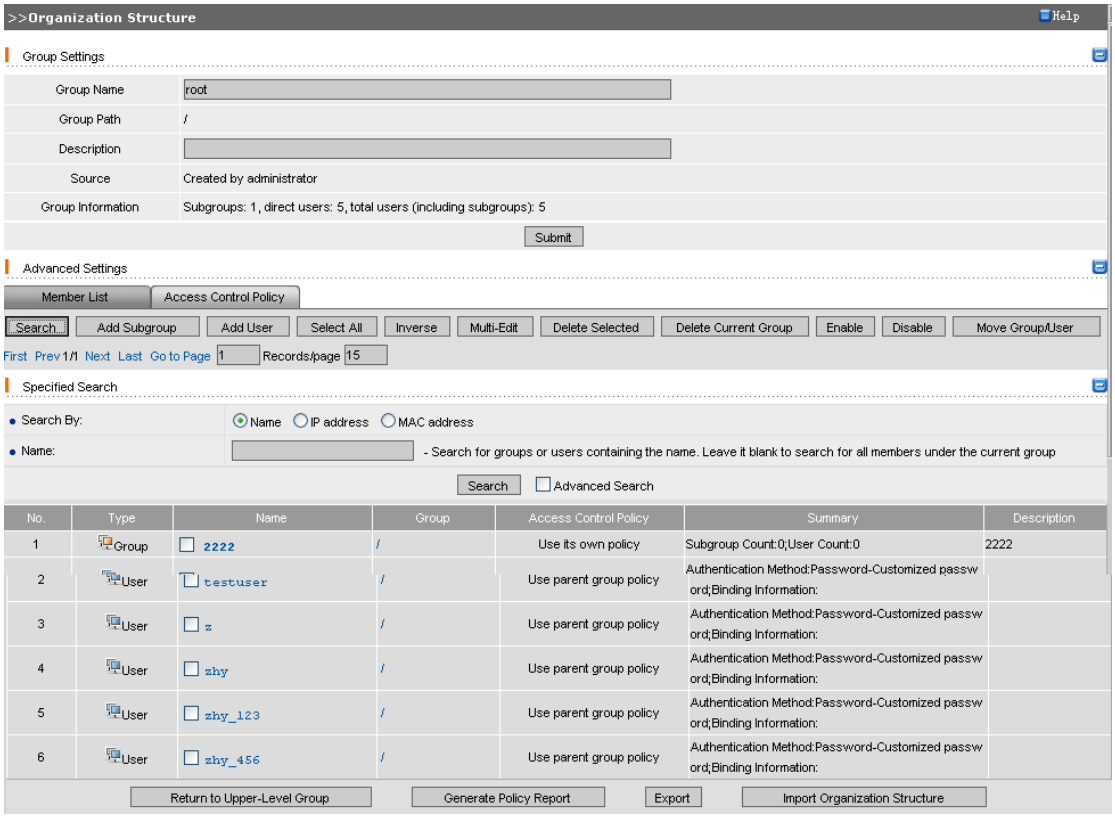
[Description]: Displays the description of each member.

<Select All>, <Inverse>: Click it to select the needed member(s) quickly.

A group is of hierarchic structure, supporting maximum 16 hierarchies.

7.4.1. Search

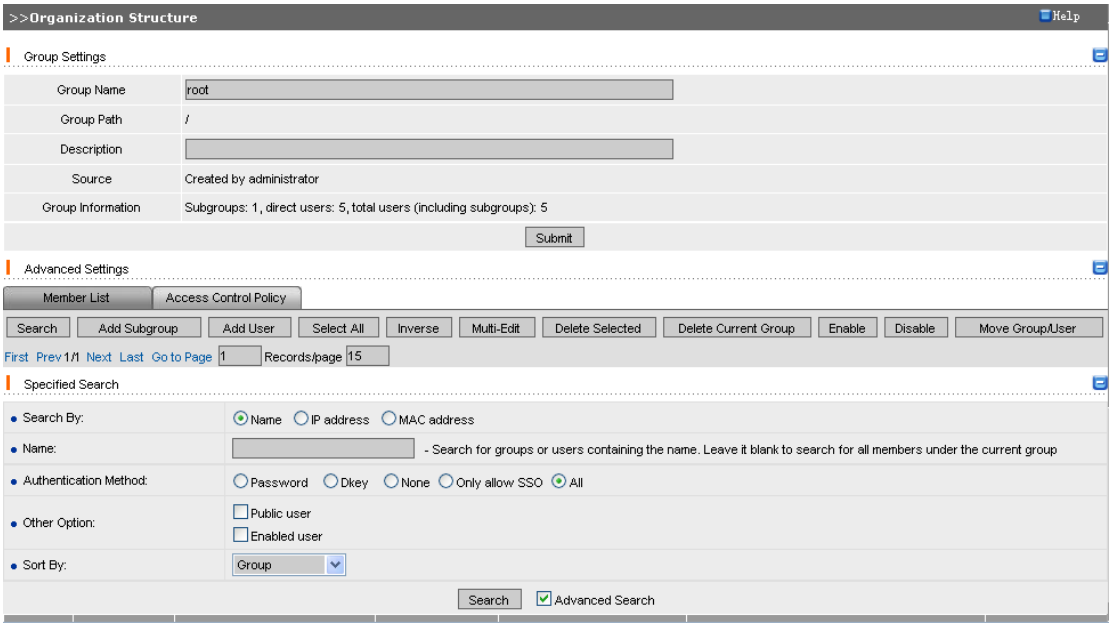
[Search]: Click this button and set the specific conditions to search for user(s) or user group(s) among the existing subgroup and users, as shown below (in this example, it searches for all the subgroups and users of the root group).



[Search By]: Configures the conditions for searching. Options are [Name], [IP address] and [MAC address], among which the [IP address] and [MAC address] are used for finding user.

[Records/page]: Configures the number of members searched and to be displayed in the list followed.

[Advanced Search]: Check this option, and the advanced search conditions appears which will help you to set more specific conditions to find a needed group or user. The advanced search conditions are [Authentication Method], [Other Option] and [Sort By].

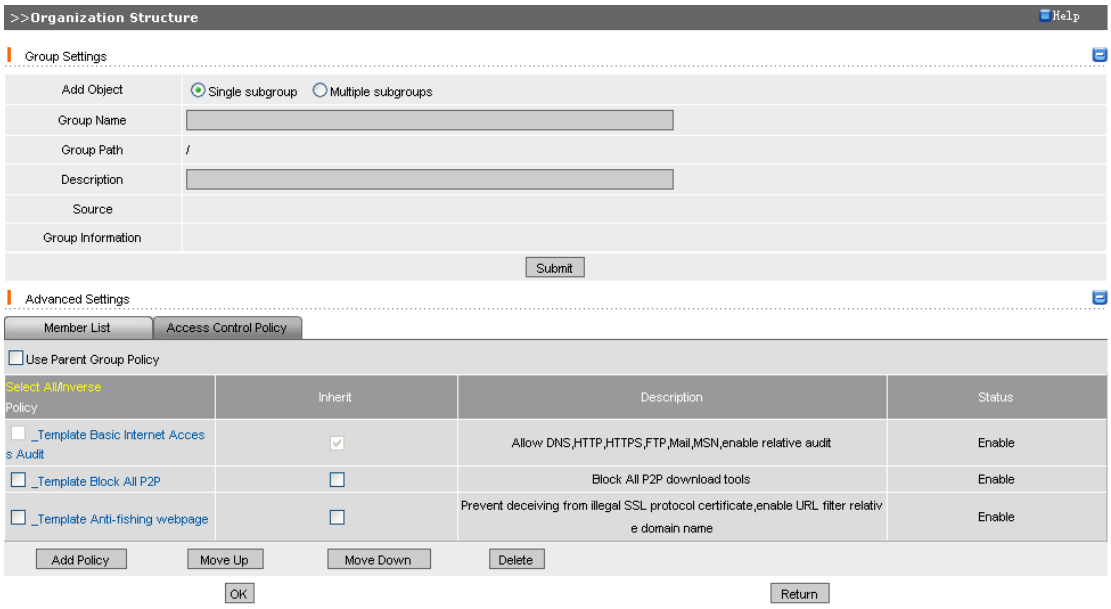


<Search>: Click this button to have the matching subgroup(s) or user(s) displayed in the list followed.

7.4.2. Add Subgroup

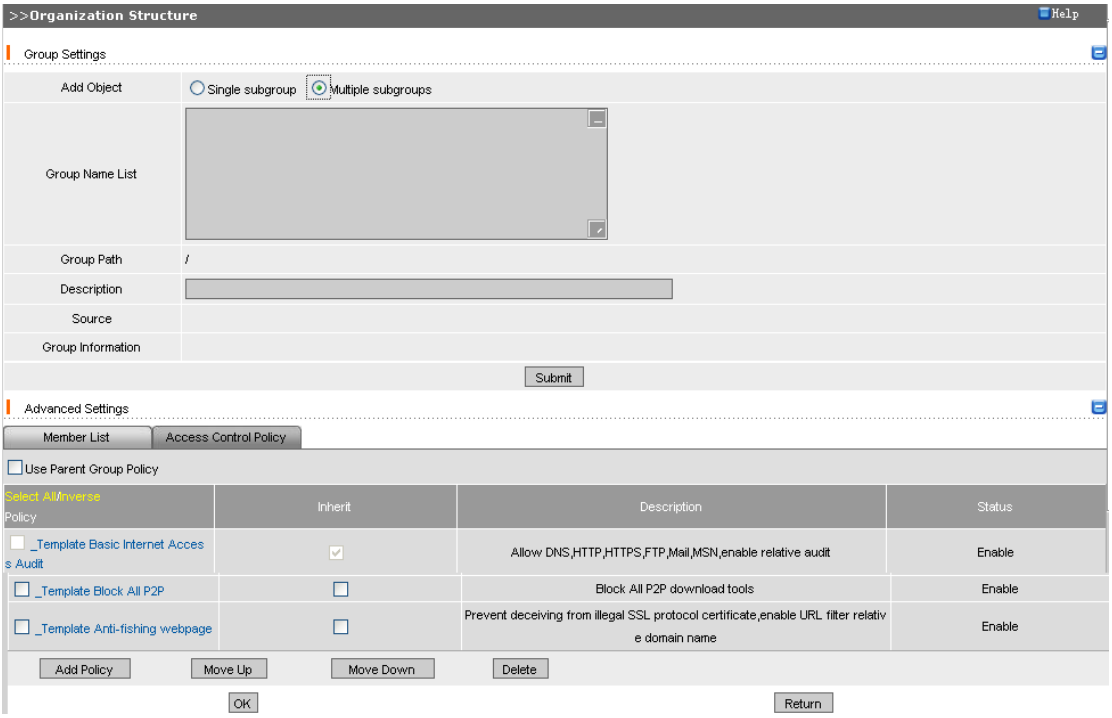
Under the [Member List] page, click the <Add Subgroup> button to add subgroup.

The configuration page is as shown below:



Add an object, [Single subgroup] or [Multiple subgroups], to add one subgroup or multiple subgroup at one time respectively.

If [Multiple subgroups] is selected, you can add a number of subgroups at a time that are of same properties. The configuration page is as shown below:

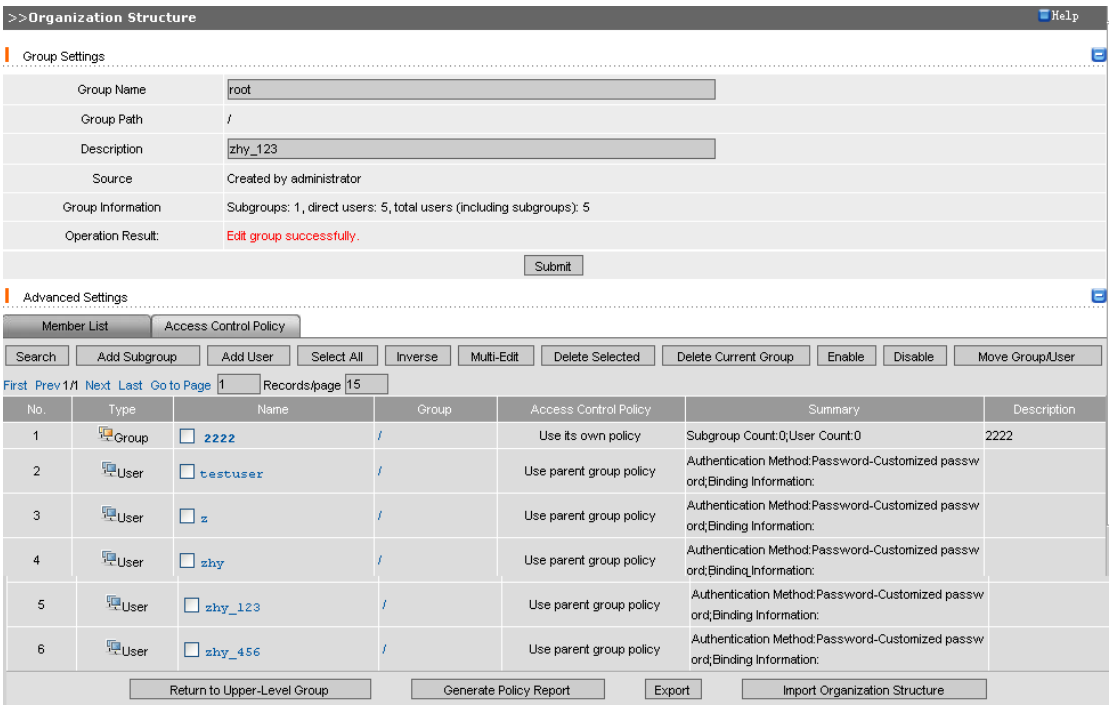


[Group Name]/[Group Name List]: Configures the name or name list of the subgroup or subgroups.

[Group Path]: Configures the path of parent group of the to-be-created subgroup. In this example, the created subgroup belongs to the root group. The path is indicated by a back slash (/).

[Description]: Type a brief introduction for this newly-created subgroup.

Then click the <Submit> button and the subgroup(s) will be added to the member list, as shown below:

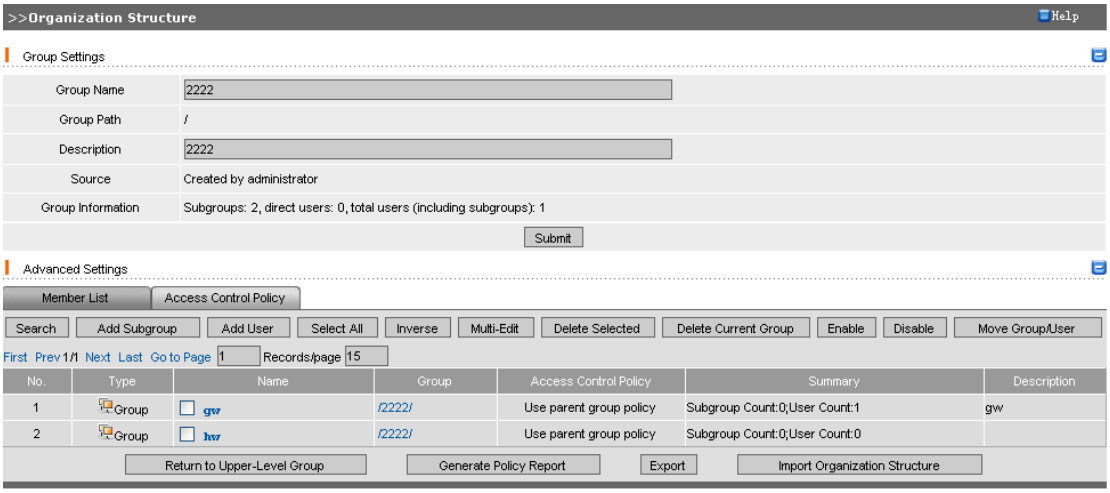


- The newly-created subgroup(s) will be displayed in the left tree, and in member list as well.
- To add a subgroup of a certain group, you have to first get into the corresponding configuration page of this group, and then click the <Add Subgroup> button and follow the instructions to add subgroup. For instance, to add a subgroup for the “2222”, you have to click [2222] (on the left tree) and then click the <Add Subgroup> button.
- The hierarchic structure of SANGFOR gateway supports maximum 16 hierarchies (root group included).

7.4.3. Edit Subgroup

Under the default configuration page of [Member List], click the name of a subgroup to get into the configuration page of this subgroup.

The configuration page is as shown below:



[Search]: The function and configuration are the same with those in the above Section [Add Subgroup]. Be noted that here you can only search the members in the group "2222". It is the same with other subgroup (searching for the members of the current subgroup).

<Add Subgroup>: Click this button to add subgroup(s) for the current group. For detailed configuration, please refer to the above section.

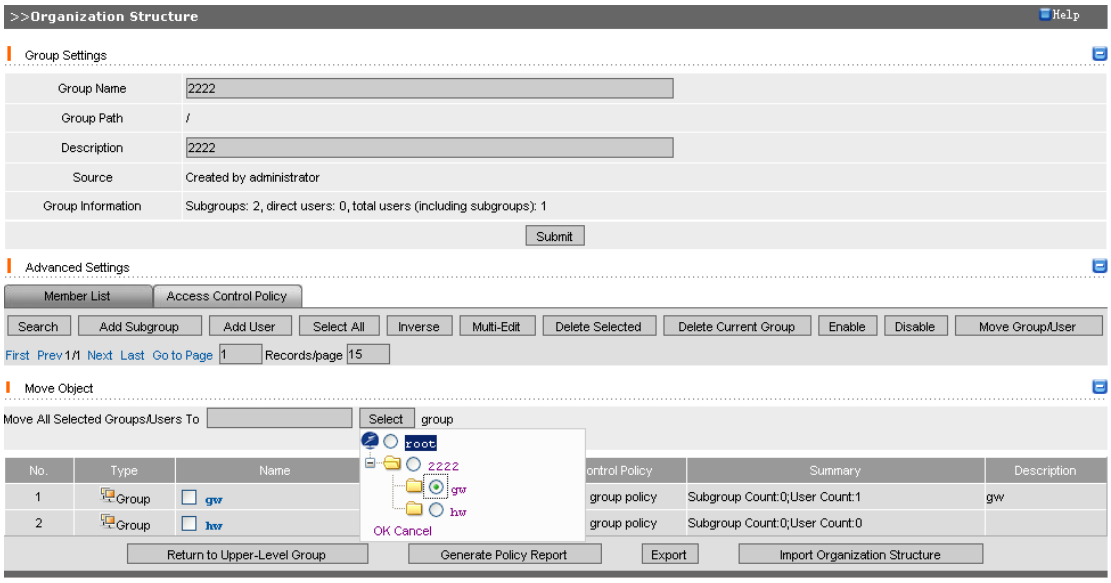
<Add User>: Click this button to add user(s) for the current group. For detailed configuration, please refer to the next section.

<Multi-Edit>: Click this button to edit the items that all of the selected member(s) have and share.

<Delete Selected>: Click this button to delete the selected subgroup(s) or user(s).

<Enable>, <Disable>: Click it to enable or disable the selected user(s).

<Move Group/User>: Click this button to move the selected group(s) or user(s) to another group. The included subgroup(s)/user(s) and access control policy/policies of the selected member will also be moved. The configuration page is as shown below:



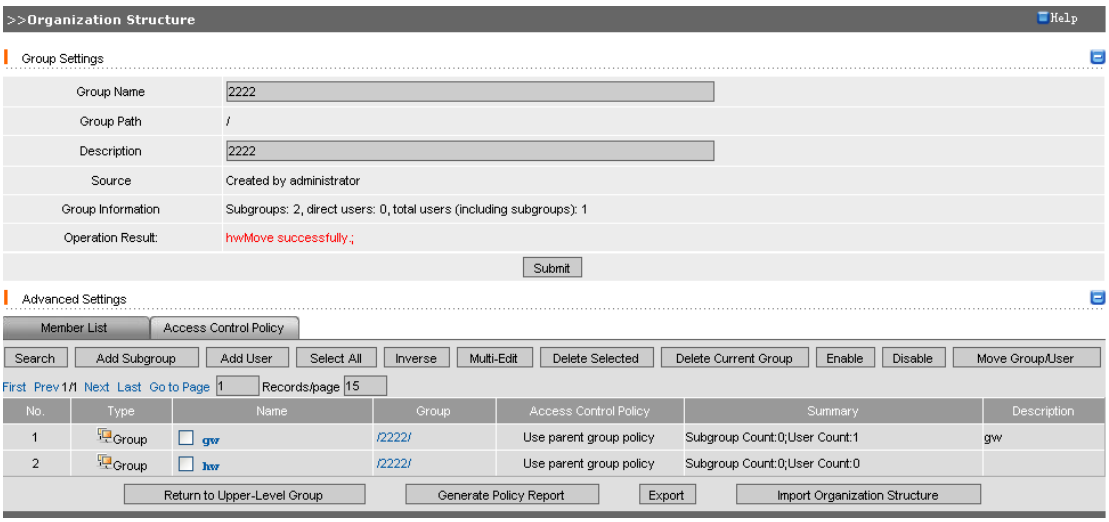
Check the needed subgroup or user(s) to be moved, and then click the <Select> button; choose a target group in the organization structure and click <OK>. The selected member(s) then is moved to the target group.

<Return to Upper-Level Group>: Click this button to back to the configuration page of its upper level group.

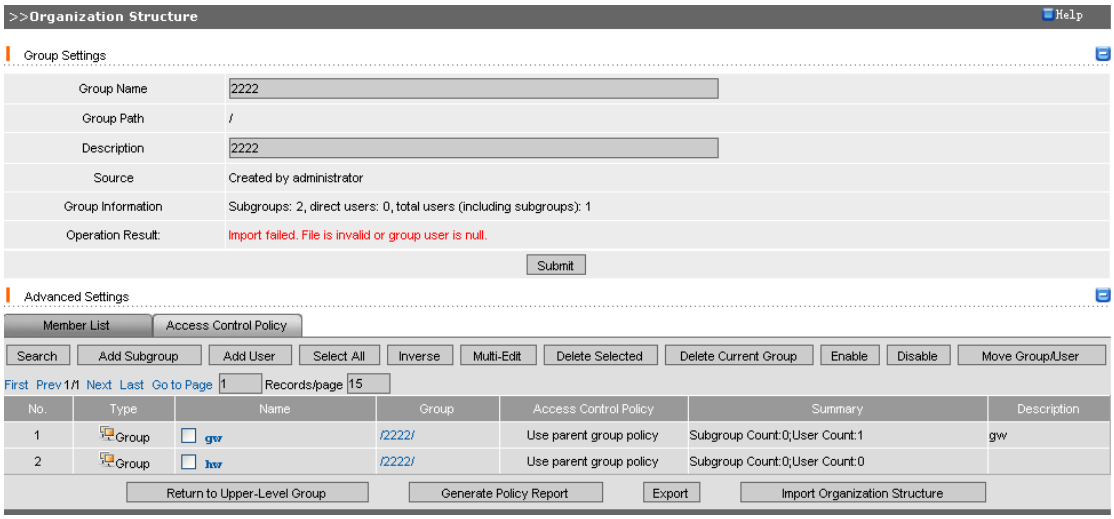
<Export>: Click it to export the structure or the members of the current group, for the purpose of saving them. The exported information includes the properties.

<Import Organization Structure>: Click it to export and import the structure or the members of the current group, for the purpose of copying them to another structure. The imported information includes the properties.

For instance, to copy the members of "*hw" to* "*2222"*, the configurations are as shown below:



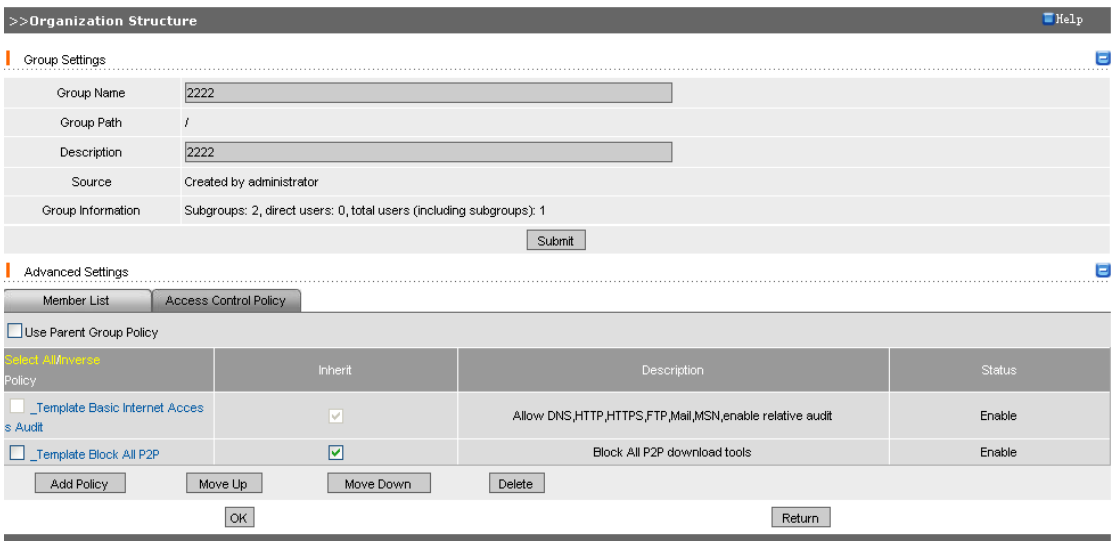
Enter the “2222” configuration page and click the <Import Organization Structure> button to import the “2222/hh”. The imported results are displayed, as shown below:



The export and import functions are only available for the subgroup members. User members cannot be exported or imported like that, for different users on the SANGFOR gateway cannot have a same name while group can share a name if only the groups are of the different paths.

[Access Control Policy] configures and manages the access control policy (policies) of the current group.

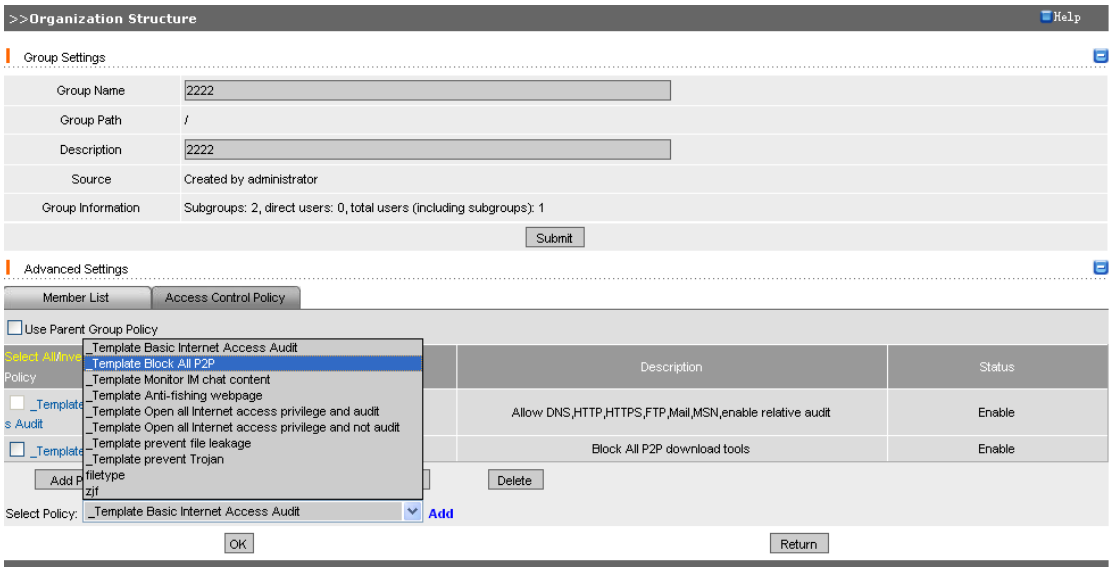
The configuration page is as shown below:



[Use Parent Group Policy]: Check this option and policy(policies) is inhered from and exactly the same with that (those) of its parent group, and you cannot do any operation on the policy(policies), such as adding, moving up/down, or deleting policy. Uncheck this option, and the group can associate with access control policy of its own.

[Select All/Inverse]: Click it to select the needed policies.

<Add Policy>: Click this button and select a policy to add it to the policy list. The configuration page is as shown below:



Select a needed policy and click <Add> to add the selected access control policy into the policy list. As to the configuration of the access control policy, please refer to Section 7.1 Access Control Policy.

<Move Up>, <Move Down>: Click it to move up or move down the selected access control policy and adjust the priority of the policies to be matched.

<Delete>: Click this button to delete the selected access control policy (policies).

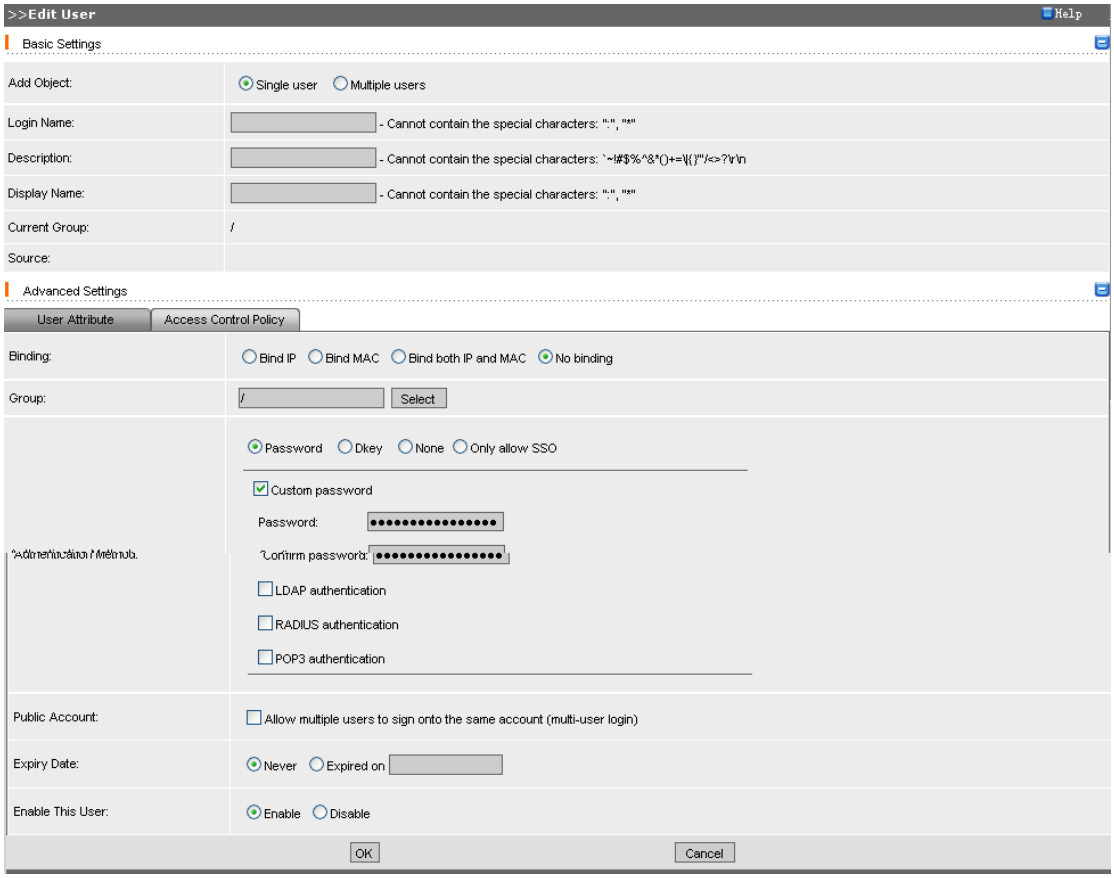
[Inherit]: Check it and this access control policy will be inherited by all of its subgroups and the users in the subgroups. The user(s) of this group also is forced to inherit this policy, however, different from the subgroup(s) of the group, this access control policy of the user(s) can be moved and deleted, while the access control policy of its subgroup cannot be moved or deleted. Among all the policies of a subgroup, the inherited policies have the higher priority over the others.

- One user or group can associate with maximum 10 access control policies.
- If there are multiple policies in the list, please adjust well the order of the policies. As to the detailed introductions and notes, please refer to Section 7.1 Access Control Policy.

7.4.4. Edit User

Under the [Member List] page, click the <Add User> button to add user(s).

The configuration page is as shown below:



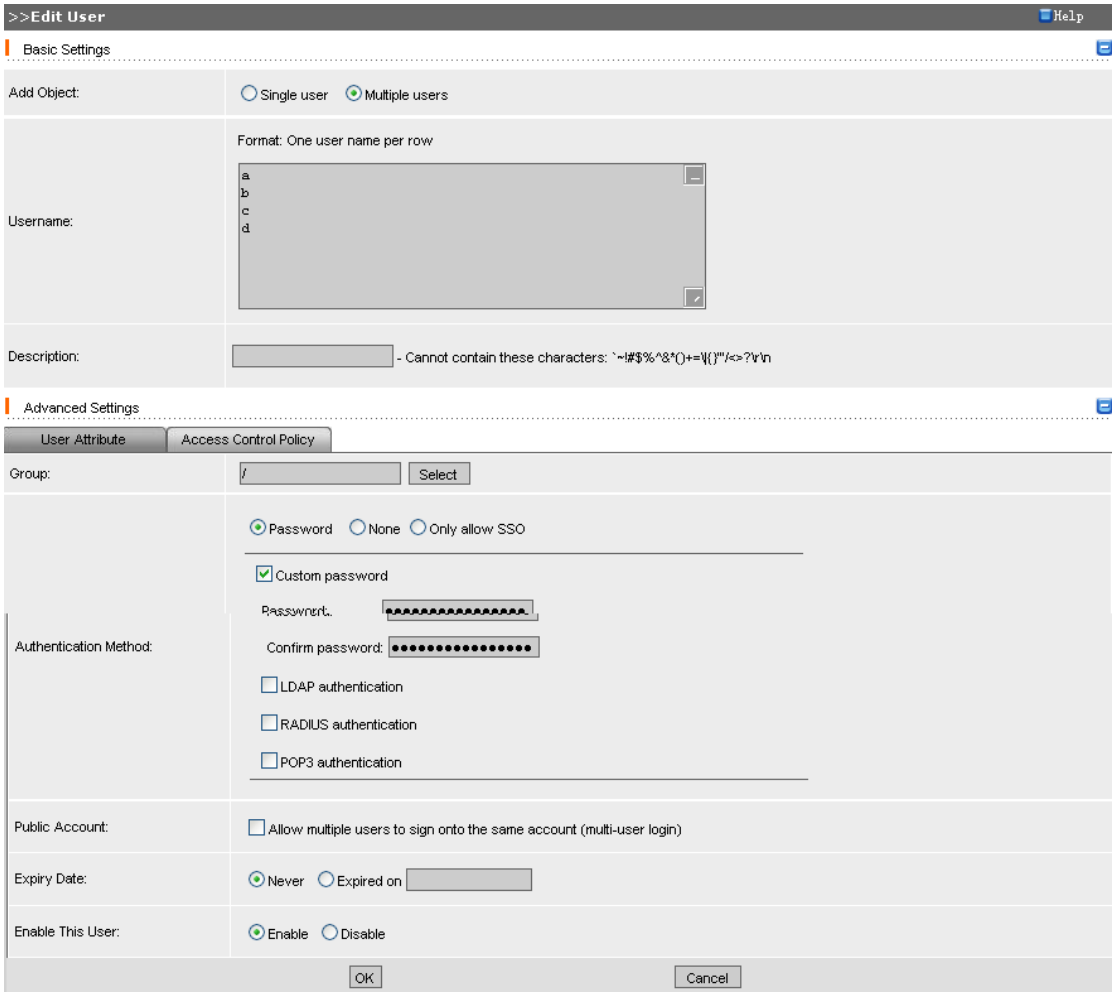
Configures [Add Object], [Single user] or [Multiple users], to add one user or multiple users at one time respectively.

[Group Path]: Configures the path of parent group of the to-be-created user. The path is indicated

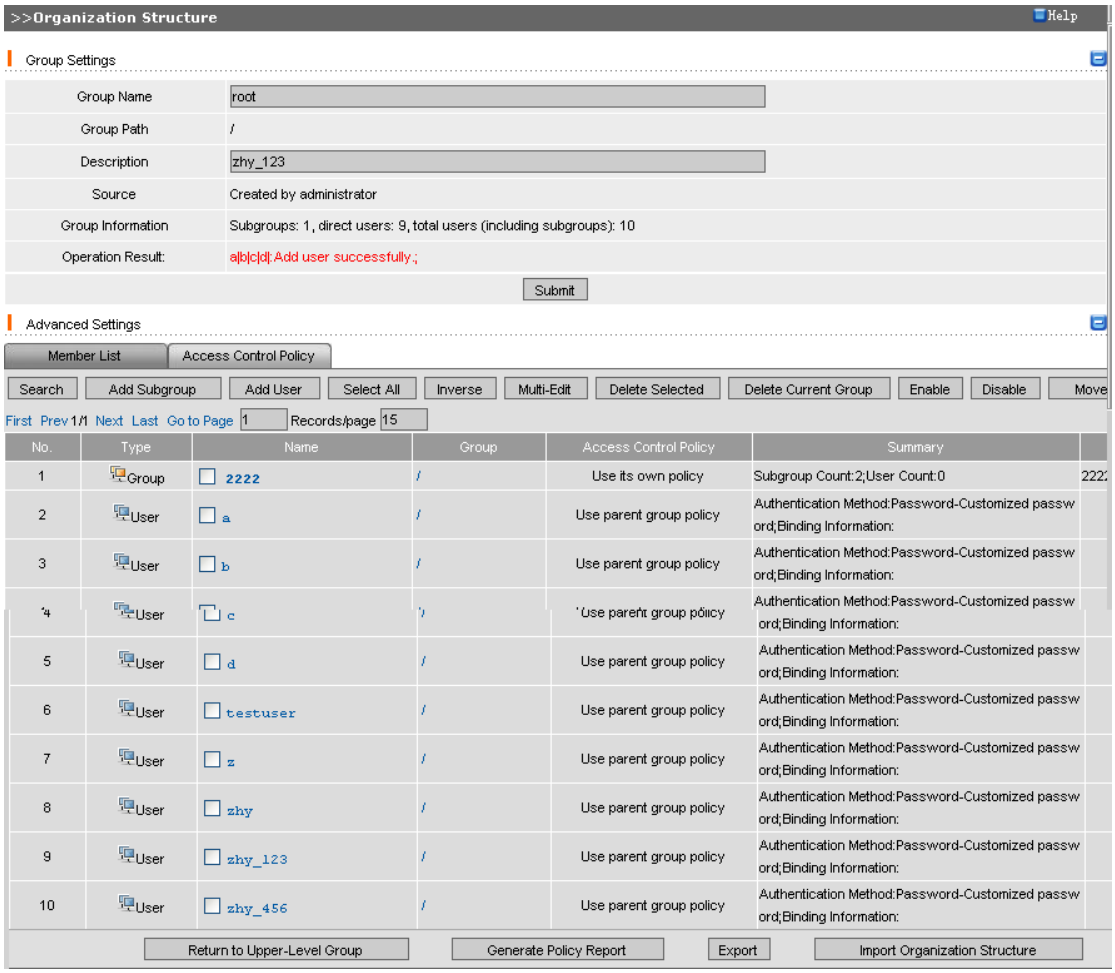
by a back slash (/).

[Description]: Type a brief introduction for this newly-created user.

If [Multiple users] is selected, you cannot configure the [Display Time], bind IP or MAC address, or create DKEY authentication user. The configuration page is as shown below:



Having completed configuring this page, you have to click the <OK> button to save the settings and add the new user, as shown below:

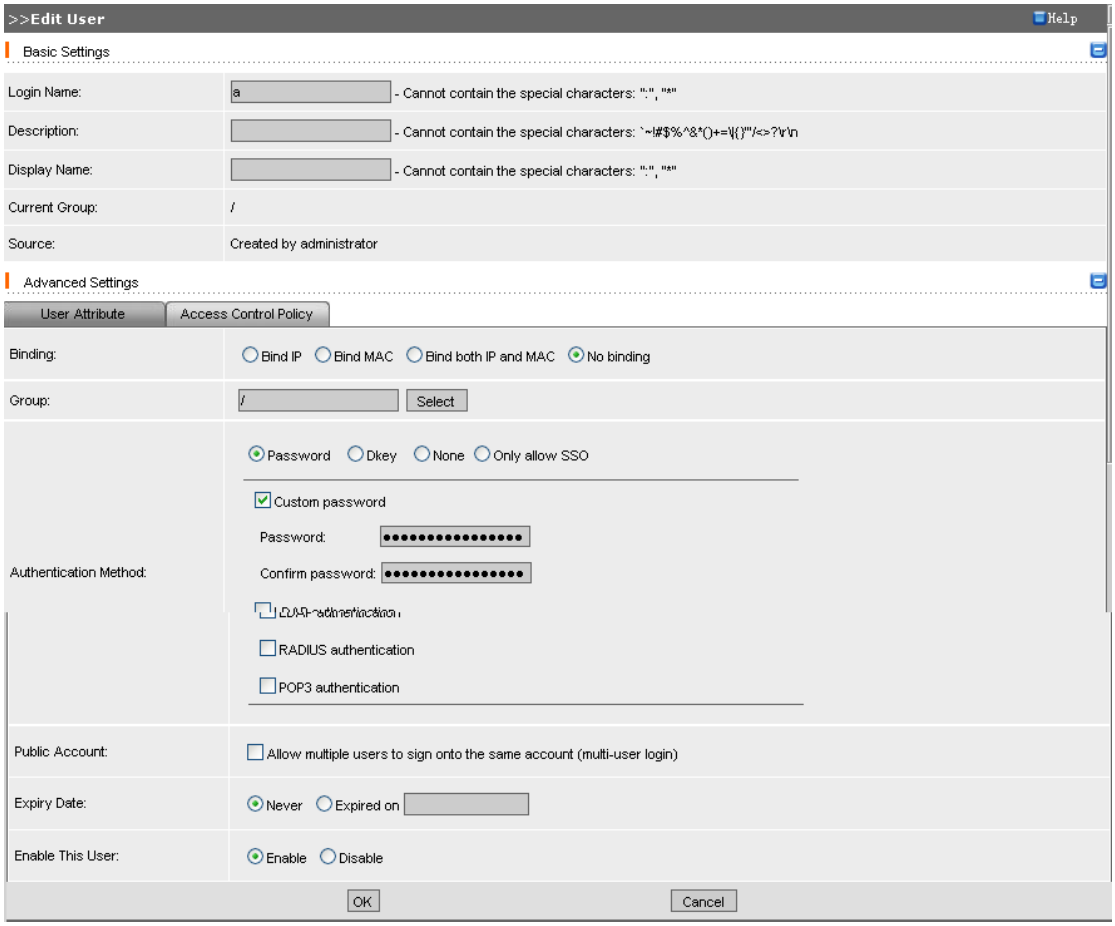

>>Organization Structure
Help
Group Settings
Group Name
root
Group Path
/
Description
zhy_123
Source
Created by administrator
Group Information
Subgroups: 1, direct users: 9, total users (including subgroups): 10
Operation Result:
a|b|c|d|:Add user successfully.;
Submit
Advanced Settings
Member List
Access Control Policy
Search
Add Subgroup
Add User
Select All
Inverse
Multi-Edit
Delete Selected
Delete Current Group
Enable
Disable
Move
First Prev 1/1 Next Last Go to Page 1 Records/page 15
No. Type Name Group Access Control Policy Summary
1 Group 2222 / Use its own policy Subgroup Count:2;User Count:0
2 User a / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
3 User b / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
4 User c / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
5 User d / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
6 User testuser / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
7 User z / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
8 User zhy / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
9 User zhy_123 / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
10 User zhy_456 / Use parent group policy Authentication Method:Password-Customized password;Binding Information:
Return to Upper-Level Group
Generate Policy Report
Export
Import Organization Structure

Till then the user is added successfully and the new user is listed in the [Member List].

7.4.5. Edit User

Under the default configuration page of [Member List], click the name of a user to get into the configuration page of this user.

The configuration page is as shown below:



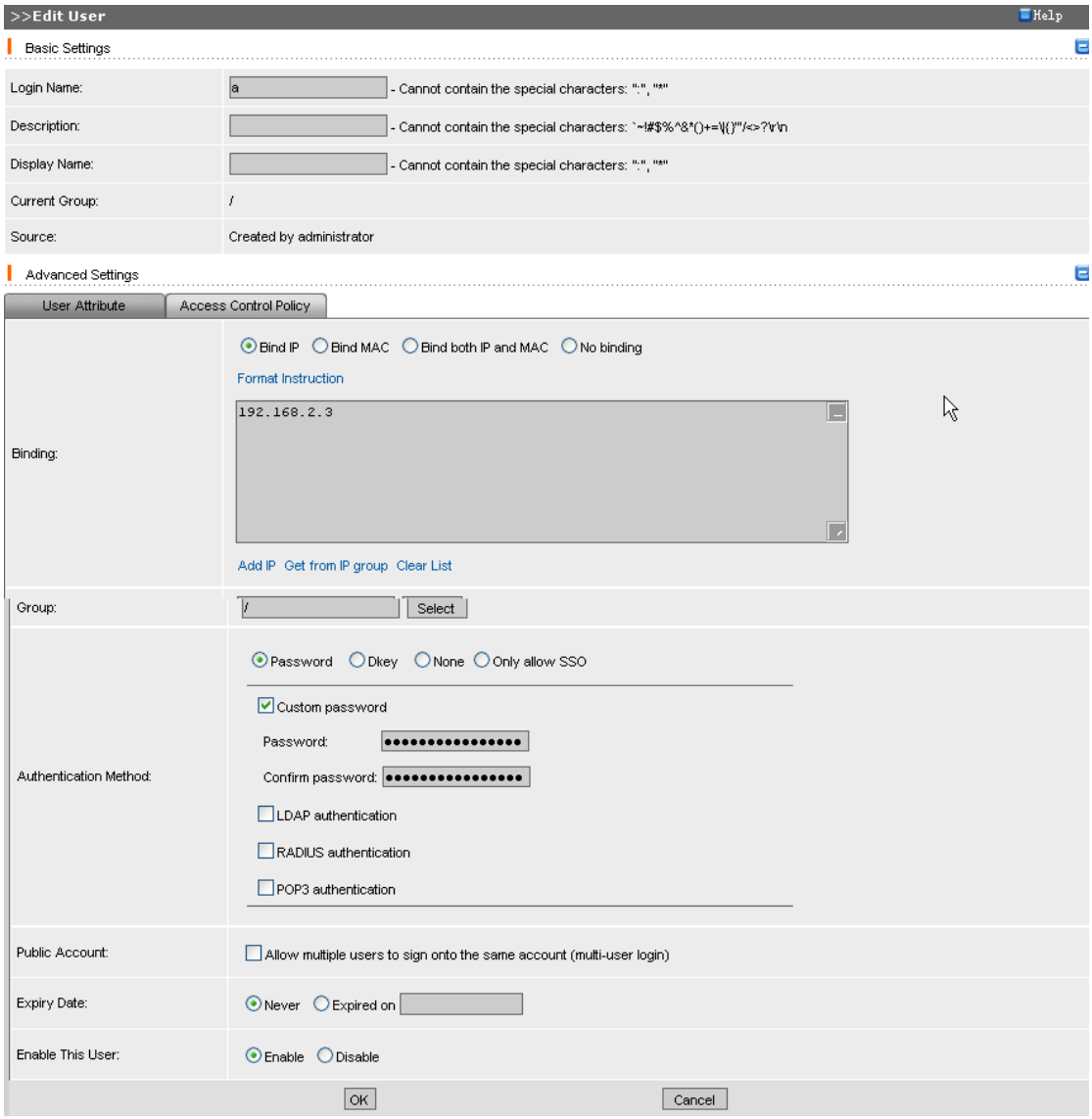
7.4.5.1. Binding IP/MAC

[Binding] configures the to-be-bound IP/MAC only with which the users can get authenticated through the IAM gateway device. Options are [Bind IP], [Bind MAC], [Bind both IP and MAC] and [No binding]. If [No binding] is selected, you have to configure an authentication method ([Password], [Dkey] or [Only allow SSO]).

You can click <Format Instruction> and view the notes for filling in and format of IP or MAC address(es).

7.4.5.1.1. Bind IP

Select [Bind IP] and configure the to-be-bound IP followed, as shown below:



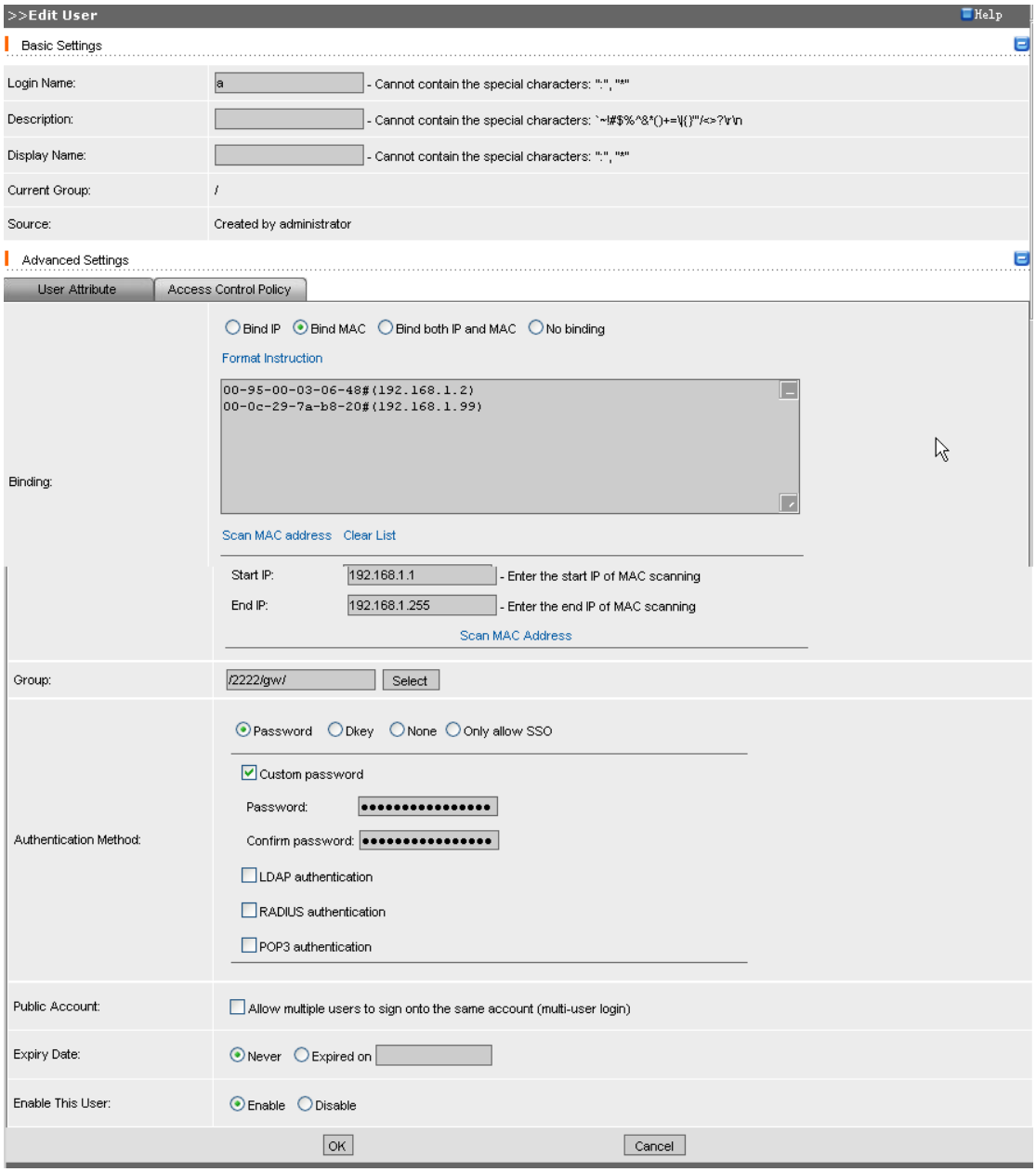
Click <Add IP>, and configure [Add Object], [Single IP], [IP range] or [Subnet], and enter an IP address or IP range respectively.

<Get from IP group>: Click it to select an already defined IP group (as to the configuration of IP group, please refer to the relevant part in Section 4.5 Schedule).

<Clear List>: Click it to clear all the IP address(es) in this list.

7.4.5.1.2. Bind MAC

[Bind MAC] configures the to-be-bound MAC address followed, as shown below:



To add MAC address, you can directly enter the MAC address(es) in [Binding] text box, or click <Scan MAC address>.

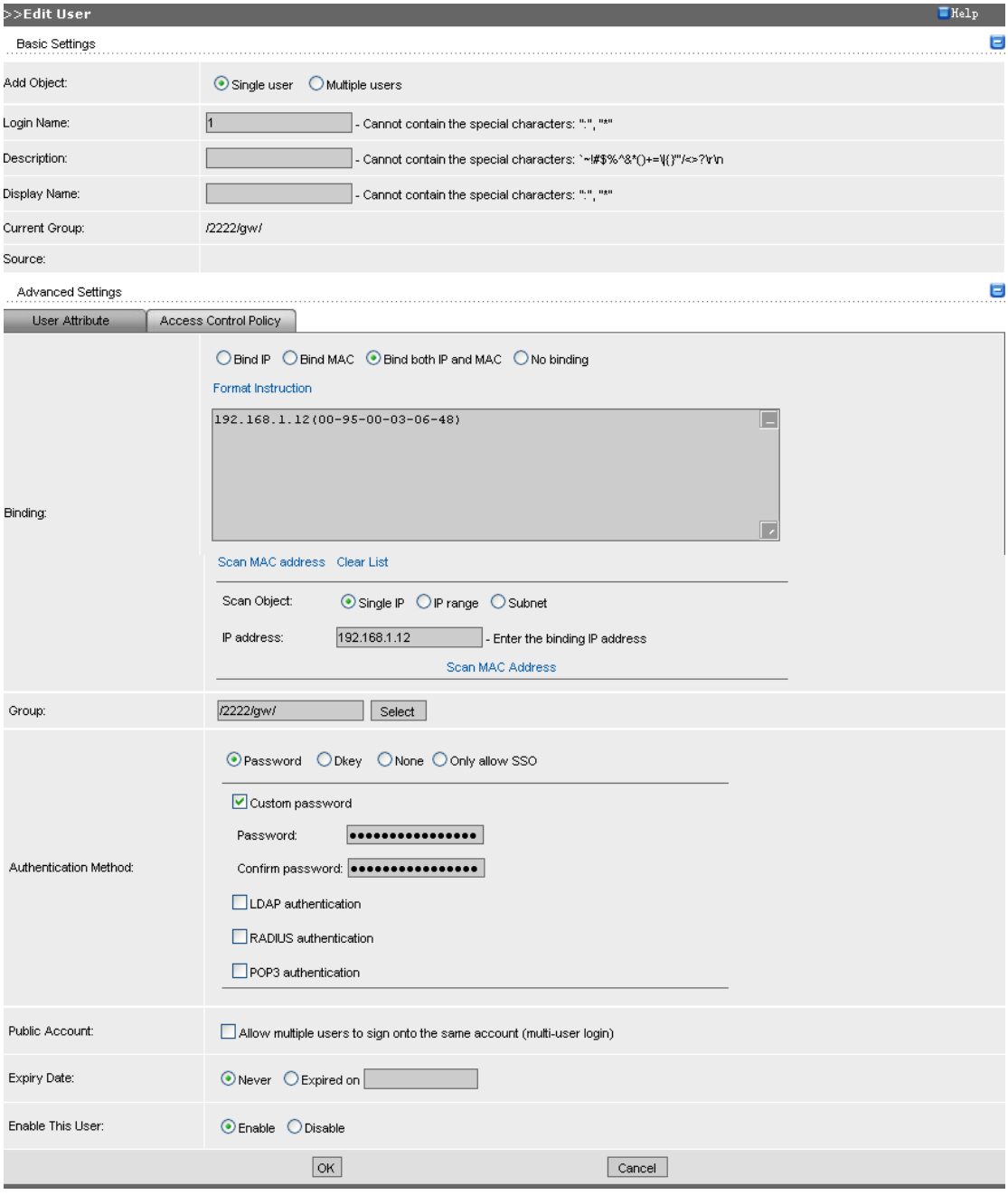
<Scan MAC address>: Click it and enter the to-be-scanned IP range, the device will scan and get the MAC addresses of these IP addresses.

<Clear List>: Click it to clear all the MAC addresses in the list.

The local device scans the MAC addresses of the configured IP addresses, applying NETBIOS protocol. The scanned IP addresses can be of different network segments, on condition that the NETBIOS protocol of the segment is enabled and that there is no firewall to block it.

7.4.5.1.3. Bind Both IP and MAC

[Bind both IP and MAC] configures the to-be-bound IP/MAC followed, as shown below:



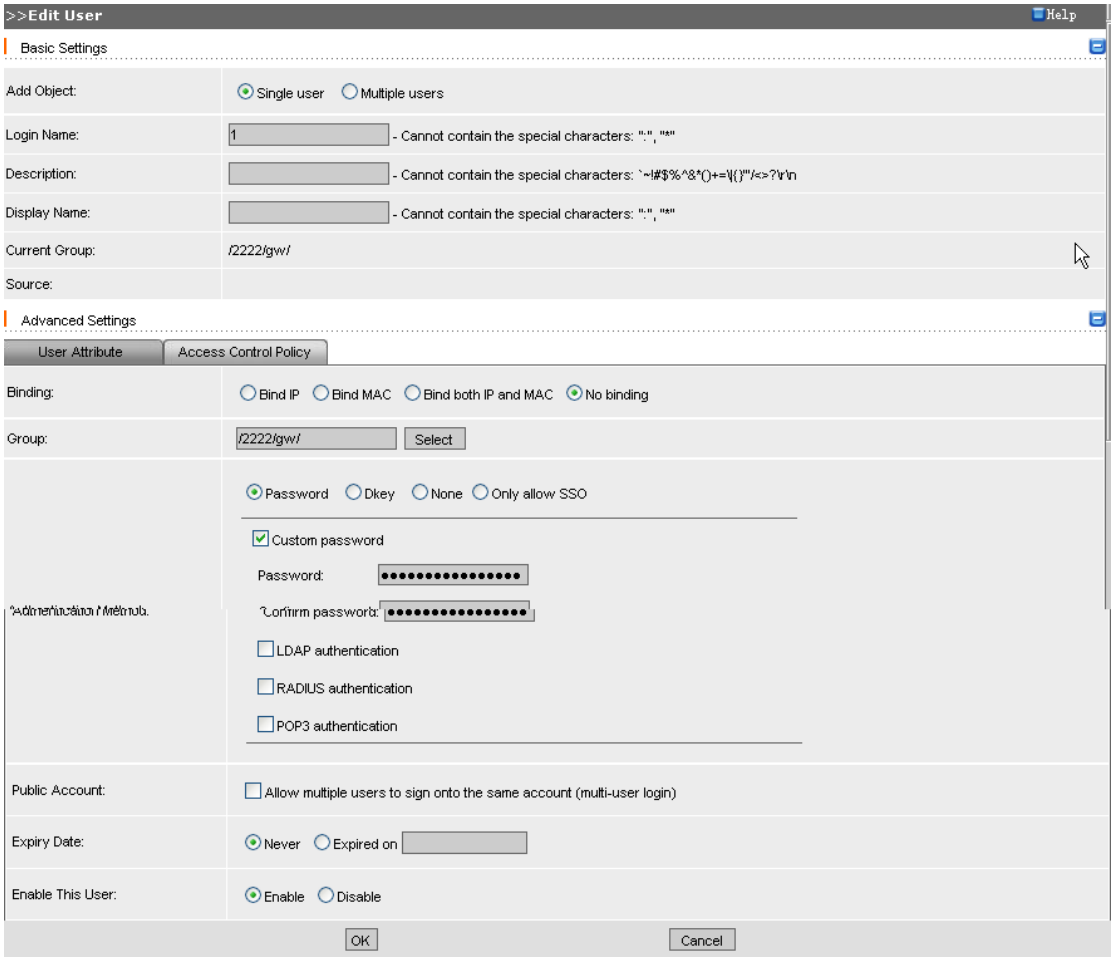
To add IP/MAC address, you can directly enter the IP/MAC address in the [Binding] text box or click <Scan MAC address>.

<Scan MAC address>: Click it and select scan object, [Single IP], [IP range] or [Subnet]; and then enter the to-be-scanned IP range, the device will scan and get the MAC addresses of these IP addresses.

<Clear List>: Click it to clear all the IP and MAC addresses in the list.

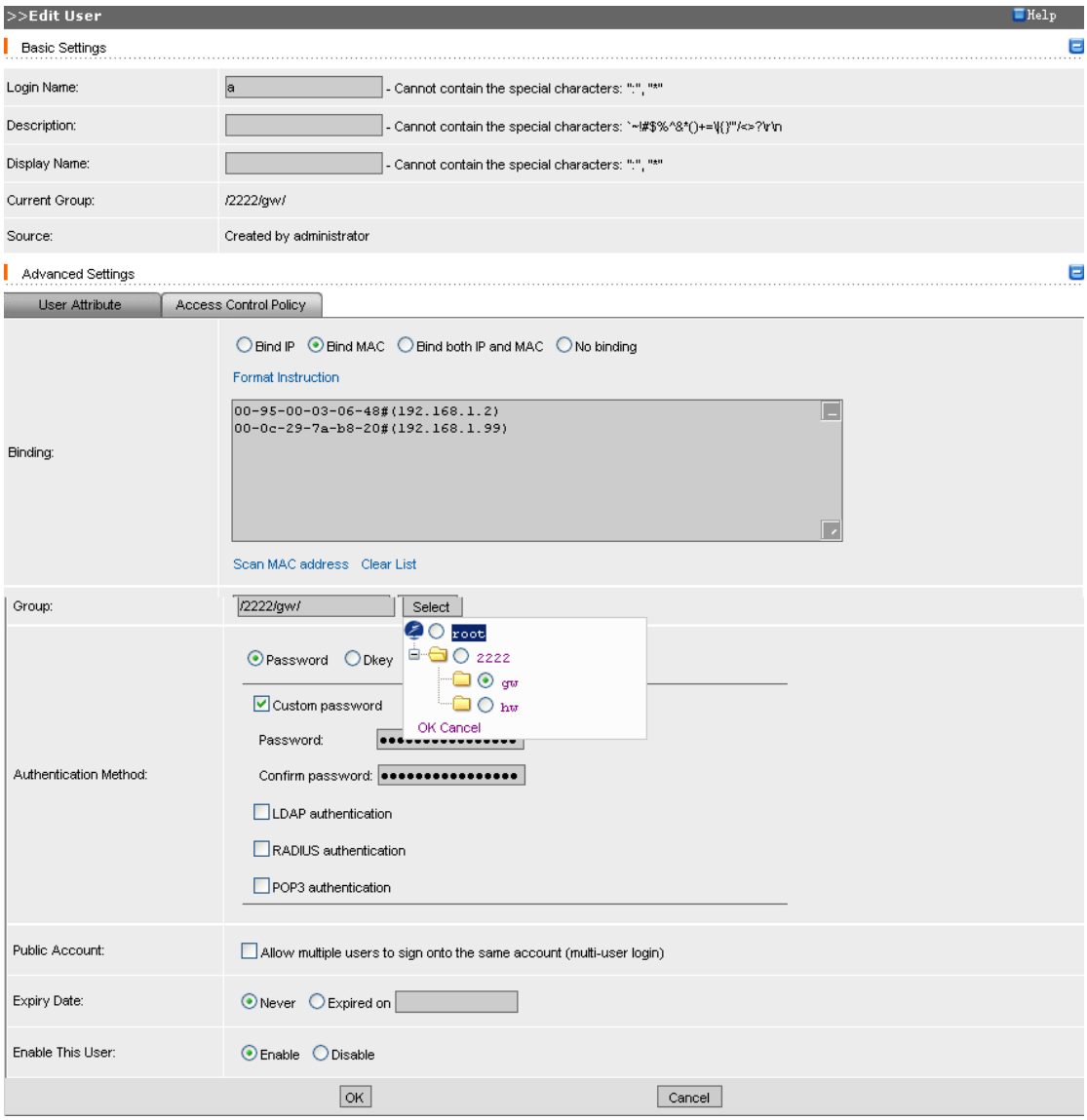
7.4.5.1.4. No Binding

[No binding] indicates not binding with any, IP address or MAC address. If this item is selected, you then have to configure at least one [Authentication Method]. The [Authentication Method] configuration options are as shown below:



7.4.5.2. Group

[Group] configures the group which the new user belongs to, as shown below:



Click the <Select> button to view the organization structure list, the user groups.

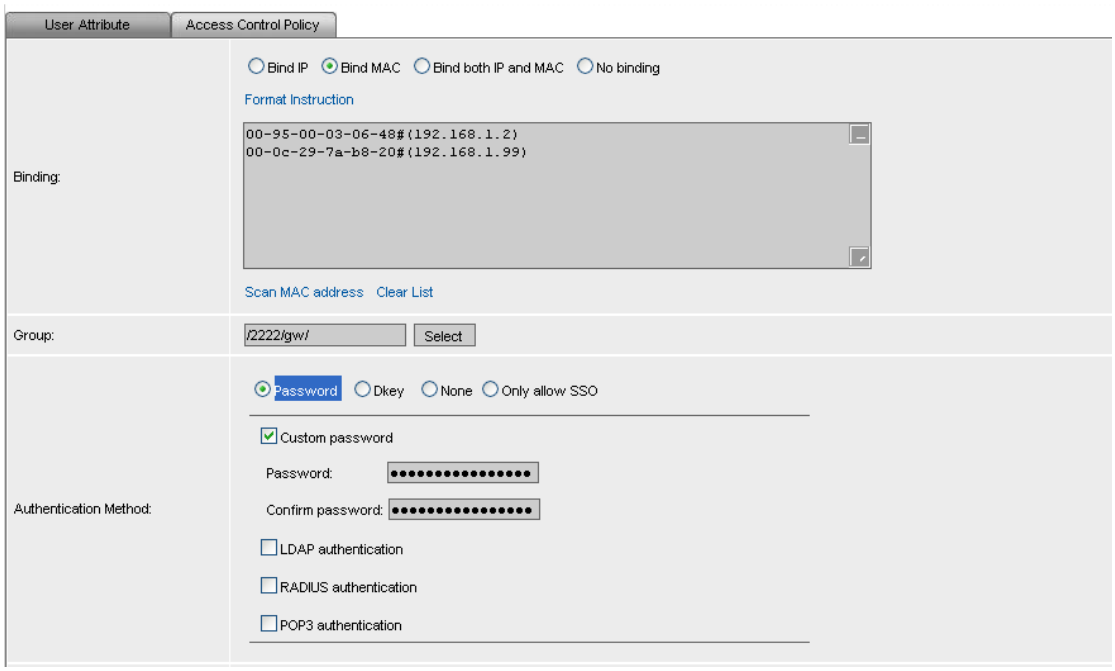
Click <OK> to add the needed and selected user group.

Click <Cancel> to give up selecting the user group.

7.4.5.3. Authentication Method

[Authentication Method] includes four options, namely, [Password], [DKEY], [None] and [Only allow SSO].

The configuration page is as shown below:



[Password]: Indicates to verify new user according to the WEB username and password.

[Custom password]: Configures the original password for the IAM gateway authenticated user (username).

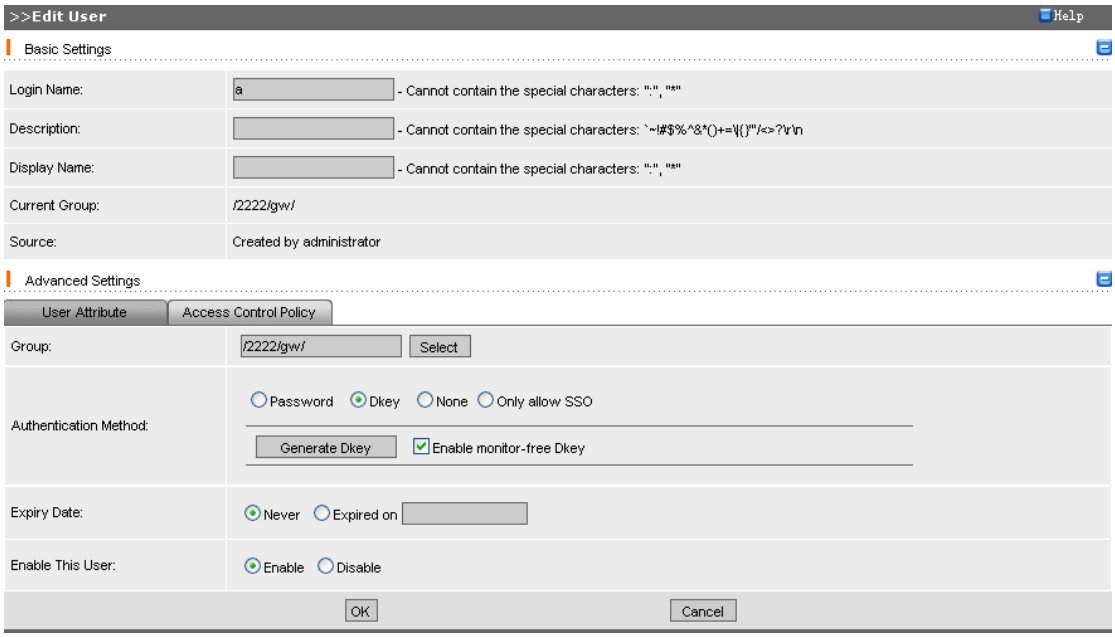
[LDAP], [RADIUS] and [POP3]: Check the server type of the third-party's that is used for authentication of this user.

You can apply multiple [Password] authentication methods to verify a user. Matching one of the authentication methods will have the user (username) get authenticated.

[DKEY]: Indicates that the user's identity is verified according to USB key. You can check [Enable monitor-free Dkey], not monitoring the users who use this authentication method.

DKEY authentication fall into two types, one is for authentication, and the other is to prevent monitoring. These two DKEY authentication types cannot be mixed up.

[Generate Dkey]: Click this button to generate the DKEY.



[Enable monitor-free Dkey]: Check this item and this user's behavior on the Internet will not be recorded (monitored).

[Dkey initial password]: Enter the initial password of the DKEY.

[Confirm password]: Enter once again the above initial password to check its correctness.

<Download Dkey Driver>: Click it to download the DKEY driver. Only when the driver is downloaded and installed will the DKEY be identified and generated.

<Start to Write Dkey>: Click this button to generate the DKEY.

[None]: Indicates that user need not enter the WEB username and password to get authenticated. If this option is selected, at least one of the binding methods should be configured, [Bind IP] or [Bind MAC].

[Only allow SSO]: Indicates that the WAN users have to get authenticated through the IAM gateway device, by meanings of SSO.

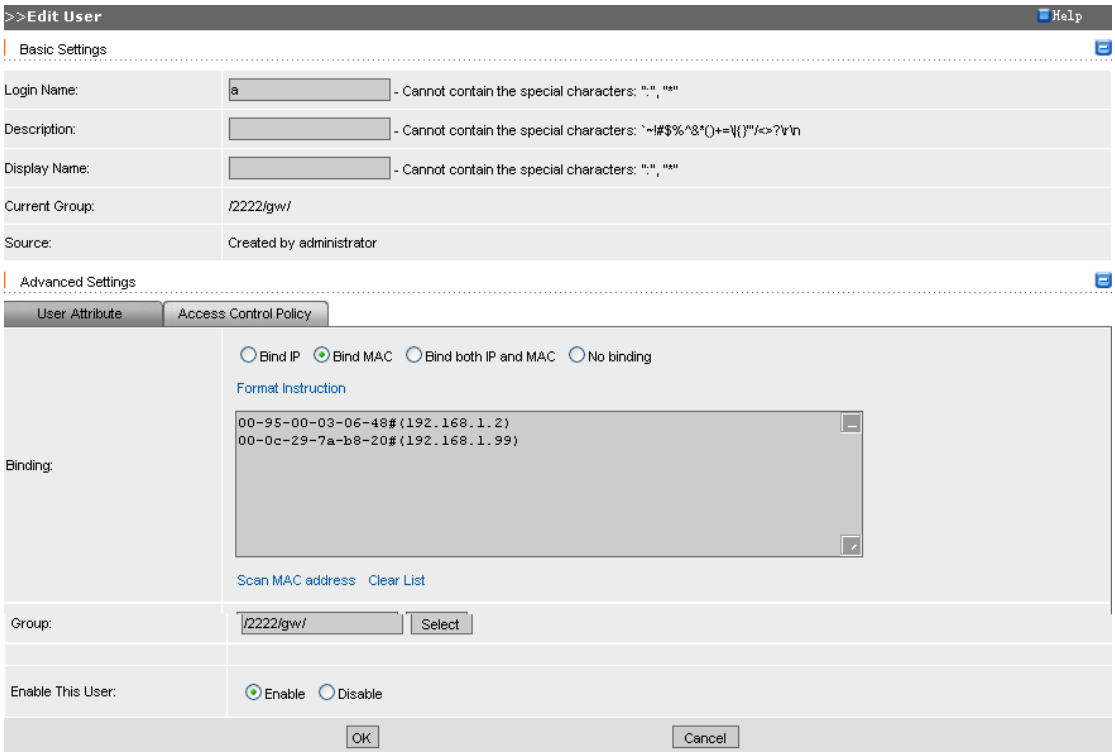
[Allow multiple users to sign onto the same account (multi-user login)]: Check this option and this account (username and password) can be used by multiple users to log on.

7.4.5.4. Expiry Date

[Expiry Date]: Two options are available. One is [Never] getting expired, and the other is [Expired

on] some day. If [Expired on] is selected, the username will get expired after the configured date. Date format is yyyy-mm-dd (for instance, 2009-06-12).

The configuration page is as shown below:



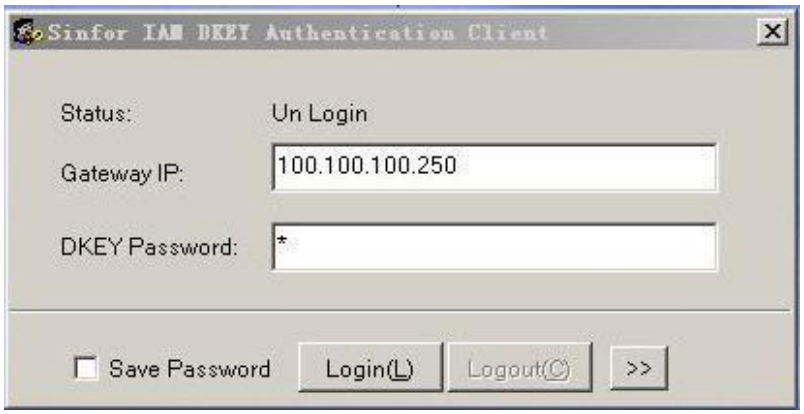
7.4.5.5. Enable This User

[Enable This User] configures whether to enable or disable this user. If [Disable] is selected, this user will get invalid.

- If more than one [Password] authentication methods (Custom password, LDAP authentication, RADIUS authentication and POP3 authentication) are checked, identity will be authenticated from top to bottom. For instance, if the four authentication methods are checked, the users have to get the [Custom password] authentication, and then the [LDAP authentication], and then the [RADIUS authentication] and finally the [POP3 authentication]; having go through the four authentications, the user need not go through any other authentication.

- Before generating DKEY, please DO download and install the DKEY driver. Inserting the DKEY, you then can click the <Generate DKEY> button.
- DKEY falls into two types, one is for authentication and the other is to prevent monitoring. These two DKEY types cannot be mixed up. If the [DKEY] is for authentication, to generate the DKEY, you must NOT check [Enable monitor-free Dkey]; if the [DKEY] is to prevent monitoring, to generate the DKEY, you must check [Enable monitor-free Dkey].
- Enter the IP address of the IAM gateway device in the IE browser and press the <Enter> key, and the [Identity Authentication system] page appears, as shown below.

Click the <DKEY client> link to download and install the DKEY client; insert the DKEY and open the DKEY client. The system requires the DKEY password; enter the password to get authenticated. If it is a monitor-free DKEY, it also clews that it is monitor-free.



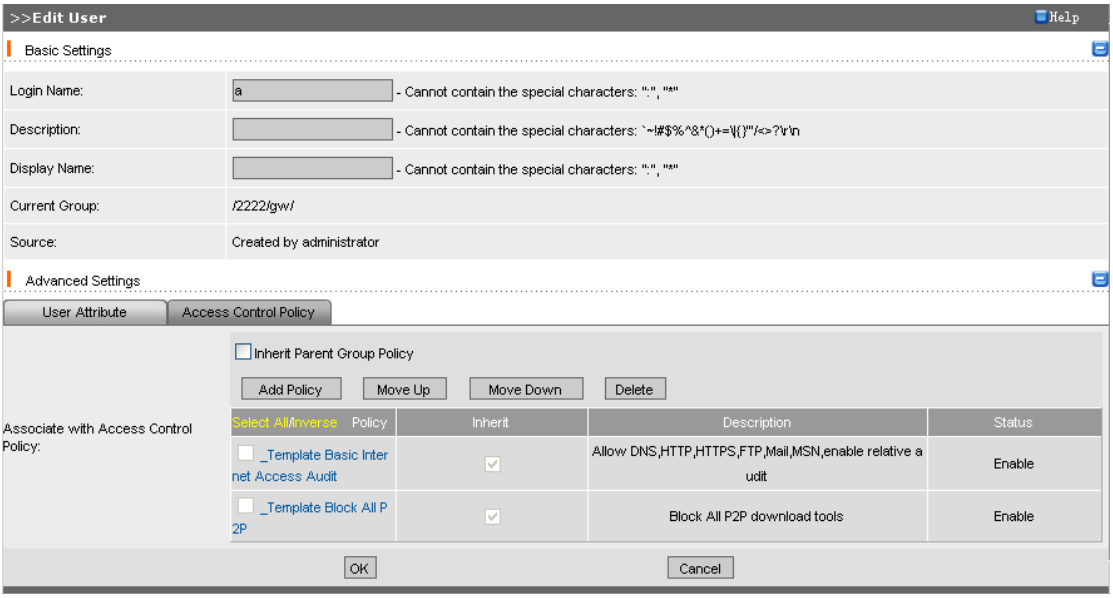
- If the [Authentication Method] is [None], either the [IP] address or [MAC] address of the

user must be bound.

- MAC addresses are scanned by the local device which applies the NETBIOS protocol. If it fails to scan the MAC address, please check whether the NETBIOS protocol of the local device is available, whether there is firewall blocking that, whether the firewall of the local device is enabled, and whether the local device is configured with multiple IP addresses.

7.4.5.6. Access Control Policy

SANGFOR IAM gateway device can configure access control policy for an individual user. Under the [Edit User] default configuration page, click [Access Control Policy], and the corresponding options appear, as shown below:



The configuration of access control policy here is the same with that in the above section (Section 7.4.3 Edit Subgroup), with the only difference that here you can configure [Inherit Parent Group Policy] because user is independent member, and cannot have its own subgroup.

As to the introduction about it, please refer to the relevant part in Section 7.4.3 Edit Subgroup.

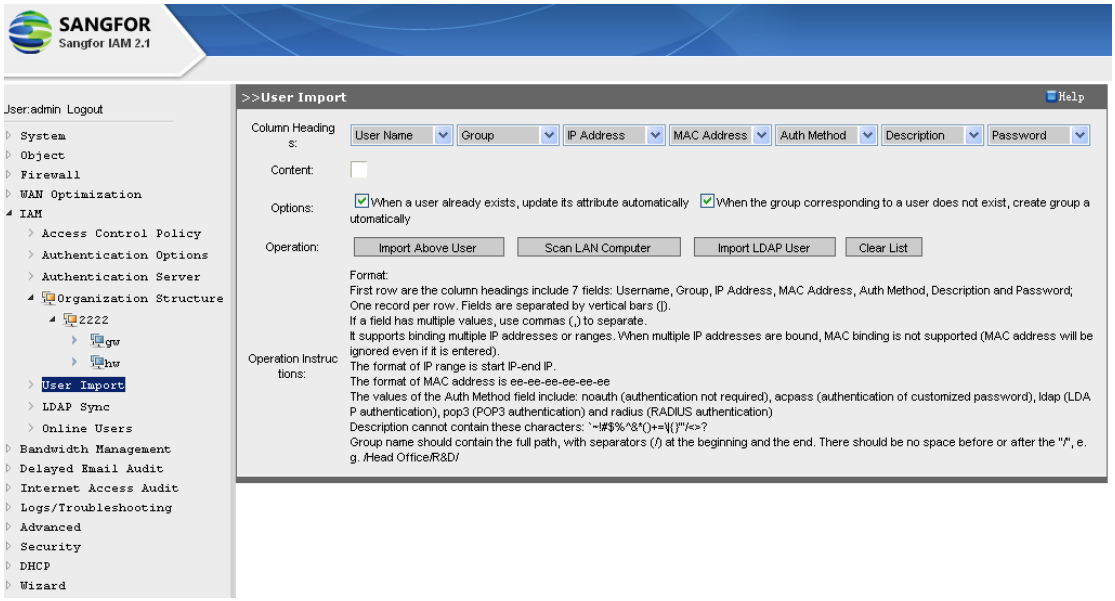
- One user or user group can associate with maximum 10 access control policies.
- As to the case that there are multiple access control policies, the matching order is as

introduced in Section 7.1 Access Control Policy.

7.5. User Import

[User Import] configuration can import batches of users.

The configuration page is as shown below:

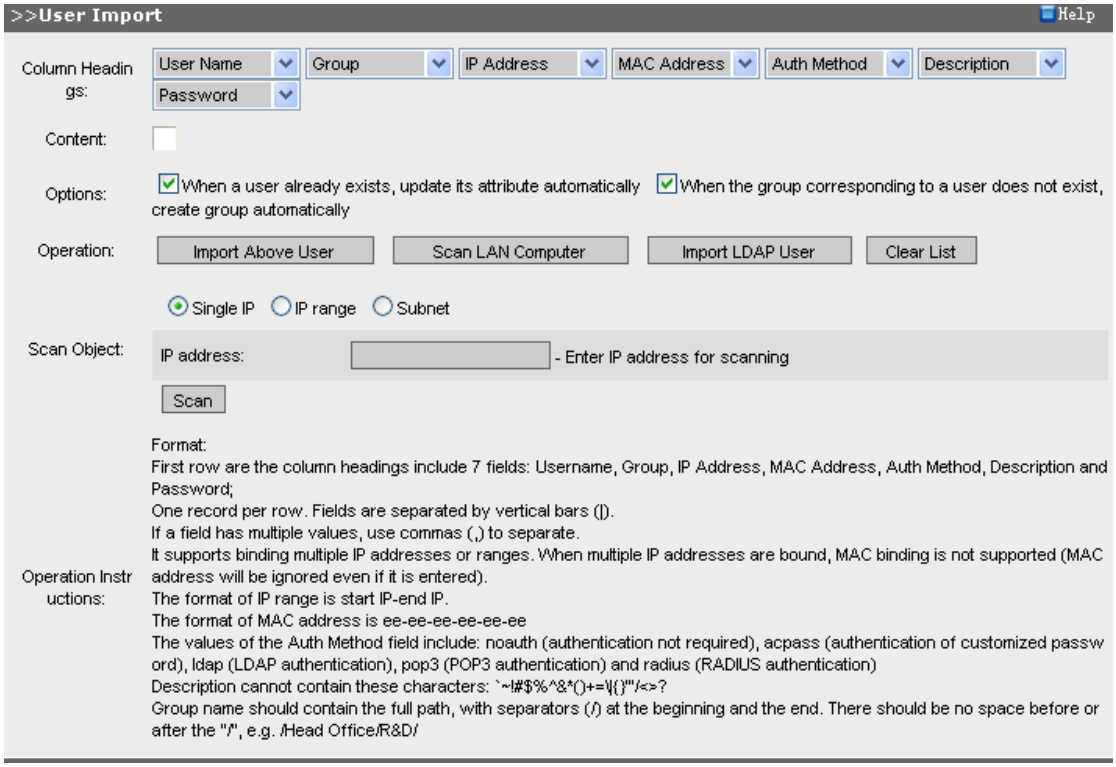

SANGFOR
Sangfor IAM 2.1
User:admin Logout
System
Object
Firewall
WAN Optimization
IAM
Access Control Policy
Authentication Options
Authentication Server
Organization Structure
2222
gw
hw
User Import
LDAP Sync
Online Users
Bandwidth Management
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Security
DHCP
Wizard
>>User Import
Help
Column Headings:
User Name
Group
IP Address
MAC Address
Auth Method
Description
Password
Content:
Options:
When a user already exists, update its attribute automatically
When the group corresponding to a user does not exist, create group automatically
Operation:
Import Above User
Scan LAN Computer
Import LDAP User
Clear List
Operation Instructions:
Format:
First row are the column headings include 7 fields: Username, Group, IP Address, MAC Address, Auth Method, Description and Password;
One record per row. Fields are separated by vertical bars (|).
If a field has multiple values, use commas (,) to separate.
It supports binding multiple IP addresses or ranges. When multiple IP addresses are bound, MAC binding is not supported (MAC address will be ignored even if it is entered).
The format of IP range is start IP-end IP.
The format of MAC address is ee-ee-ee-ee-ee-ee
The values of the Auth Method field include: noauth (authentication not required), acpass (authentication of customized password), ldap (LDAP authentication), pop3 (POP3 authentication) and radius (RADIUS authentication)
Description cannot contain these characters: `~!#$%^&*()+=\{}'"/<>?
Group name should contain the full path, with separators (/) at the beginning and the end. There should be no space before or after the "/", e.g. /Head Office/R&D/

[Column Headings] defines the columns of the user table. It supports importing the information of [User Name], [Group], [IP Address], [MAC Address], [Auth Method] (authentication method), [Description] and [Password].

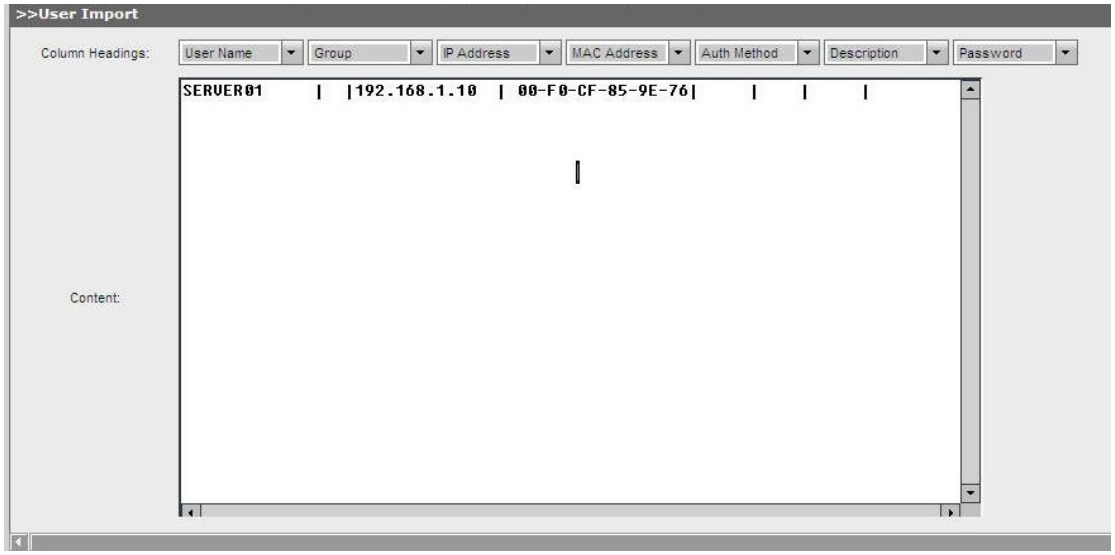
[Content] defines the record (one entry per row). Different fields are separated from each other by a vertical bar (|), including the case that the field is blank. If one field has several values, such as several IP addresses, they are separated from each other by a comma (,).

[Option]: Check [When a user already exists, update its attribute automatically] to automatically update the attribute information of the user who already exists in the user list; or check [When the group corresponding to a user does not exist, create group automatically] and this new group will be added to the member list (user list).

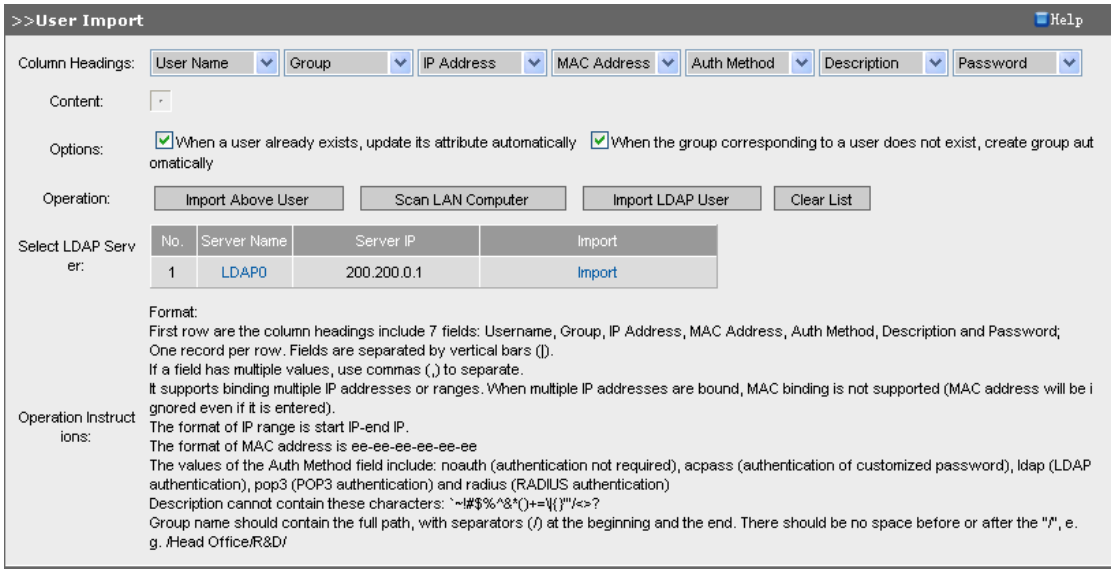
[Operation]: Click the <Import Above User> button to import the user and attribute in the [Content]. Or click the <Scan LAN Computer> button to view the [Scan Object], as shown below:


>>User Import
Help
Column Headings:
User Name
Group
IP Address
MAC Address
Auth Method
Description
Password
Content:
Options:
When a user already exists, update its attribute automatically
When the group corresponding to a user does not exist, create group automatically
Operation:
Import Above User
Scan LAN Computer
Import LDAP User
Clear List
Single IP
IP range
Subnet
Scan Object:
IP address:
- Enter IP address for scanning
Scan
Operation Instructions:
Format:
First row are the column headings include 7 fields: Username, Group, IP Address, MAC Address, Auth Method, Description and Password;
One record per row. Fields are separated by vertical bars (|).
If a field has multiple values, use commas (,) to separate.
It supports binding multiple IP addresses or ranges. When multiple IP addresses are bound, MAC binding is not supported (MAC address will be ignored even if it is entered).
The format of IP range is start IP-end IP.
The format of MAC address is ee-ee-ee-ee-ee-ee
The values of the Auth Method field include: noauth (authentication not required), acpass (authentication of customized password), ldap (LDAP authentication), pop3 (POP3 authentication) and radius (RADIUS authentication)
Description cannot contain these characters: `~!#$%^&*()+=\|{}'"/<>?
Group name should contain the full path, with separators (/) at the beginning and the end. There should be no space before or after the "/", e.g. /Head Office/R&D/

As shown in the above figure, you can import users according to [Single IP], [IP range] or [Subnet]. Filling in the corresponding information, you can click the <Scan> button, and the host name, IP and MAC addresses will be displayed in the [Content] table.



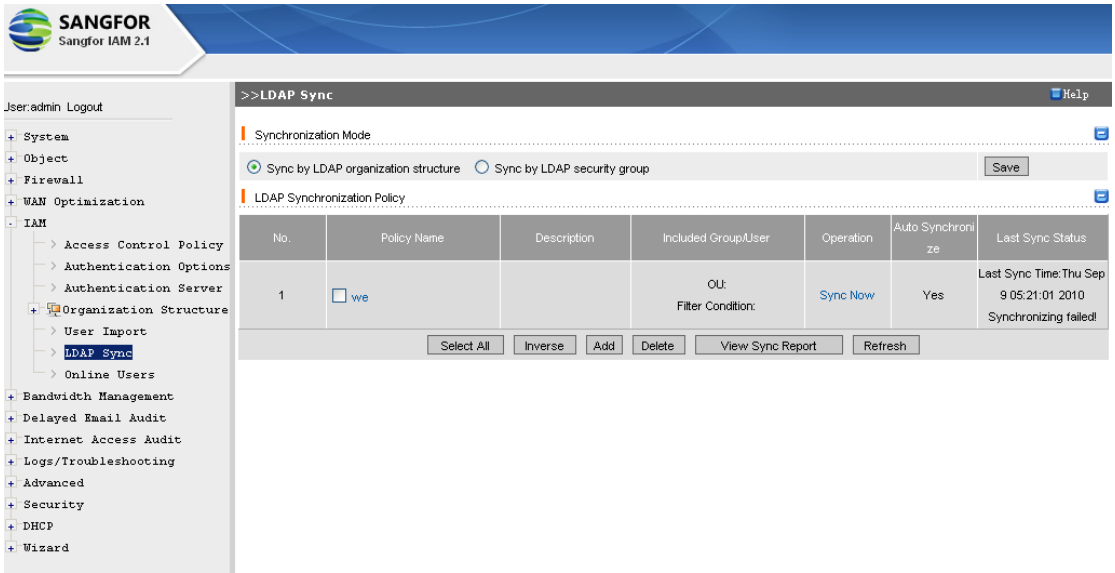
Or click the <Import LDAP User> button and the [Select LDAP Server] appears, as shown below:


>>User Import
Help
Column Headings:
User Name
Group
IP Address
MAC Address
Auth Method
Description
Password
Content:
Options:
When a user already exists, update its attribute automatically
When the group corresponding to a user does not exist, create group automatically
Operation:
Import Above User
Scan LAN Computer
Import LDAP User
Clear List
Select LDAP Server:
No.
Server Name
Server IP
Import
1
LDAP0
200.200.0.1
Import
Operation Instructions:
Format:
First row are the column headings include 7 fields: Username, Group, IP Address, MAC Address, Auth Method, Description and Password;
One record per row. Fields are separated by vertical bars (|).
If a field has multiple values, use commas (,) to separate.
It supports binding multiple IP addresses or ranges. When multiple IP addresses are bound, MAC binding is not supported (MAC address will be ignored even if it is entered).
The format of IP range is start IP-end IP.
The format of MAC address is ee-ee-ee-ee-ee-ee
The values of the Auth Method field include: noauth (authentication not required), acpass (authentication of customized password), ldap (LDAP authentication), pop3 (POP3 authentication) and radius (RADIUS authentication)
Description cannot contain these characters: `~!#$%^&*()+=\|{}'":/<>?
Group name should contain the full path, with separators (/) at the beginning and the end. There should be no space before or after the "/", e.g. /Head Office/R&D/

The LDAP server configured in [Authentication Server] will be displayed here. Click the <Import> button and the list of all the users appear.

7.6. LDAP Sync

[LDAP Sync] is used for synchronizing the users and organization structure of the domain server to the IAM gateway device, and for realizing the automatic synchronization of the user and organization structure of the domain server. Presently, this function only supports MS SGtive Directory. It falls into two synchronization modes, namely, [Sync by LDAP organization structure] and [Sync by LDAP security group].



[Synchronization Mode] configures the mode of LDAP synchronization. These two modes cannot work at the same time; you can select either of them.

Having selected one of the modes, you have to click the <Save> button followed to save the settings.

<Select All>, <Inverse>: Click it to select the needed policy or policies.

<Add>: Click it to enter the [LDAP Synchronization Policy] configuration page.

<Delete>: Click it to delete the selected LDAP synchronization policy or policies.

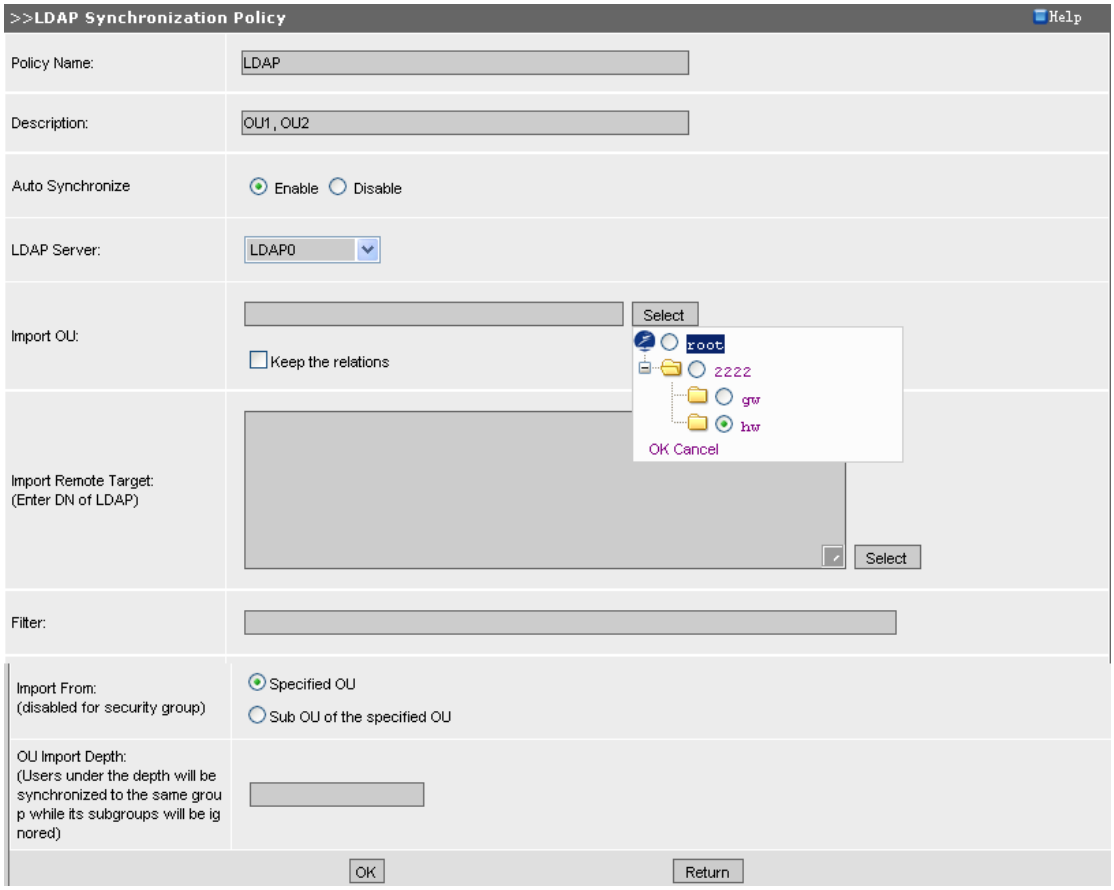
<View Sync Report>: Click it to view the LDAP synchronization report.

<Refresh>: Click it to refresh manually and view the synchronization status.

7.6.1. Sync by LDAP Organization Structure

[Sync by LDAP organization structure] synchronization mode imports the users/user groups according to the organization unit (OU) and structure of the Active Directory.

Select [Sync by LDAP organization structure], and click the <Add> button and the [LDAP Synchronization Policy] configuration page appears, as shown below:



[Policy Name]: Type a unique name for this synchronization policy.

[Description]: Type a brief introduction for this synchronization policy.

[Auto Synchronize]: Configures whether to automatically synchronize the information or not. Select [Enable] and the device will synchronize the domain users/user groups at certain time during 0:00~5:00 o'clock; select [Disable] and the device will not synchronize the users/user groups.

[LDAP Server]: Configures the domain server that is to be synchronized. As to the configuration of domain server, please refer to Section 7.3.1 LDAP.

[Import OU]: Configures the user group path (in the IAM gateway device) to which the synchronized users and organization structure are imported to. Click the <Select> button to view the organization structure of the IAM gateway device, select a group/subgroup and then click the <OK> button.

[Keep the relations]: Check this option, and the DC of the domain server will be imported together with the user and user groups.

[Import Remote Target]: Configures the organization unit (OU) of the domain server. Click the <Select> button to view the organization structure (in unit of OU) of the domain server and select a needed OU.

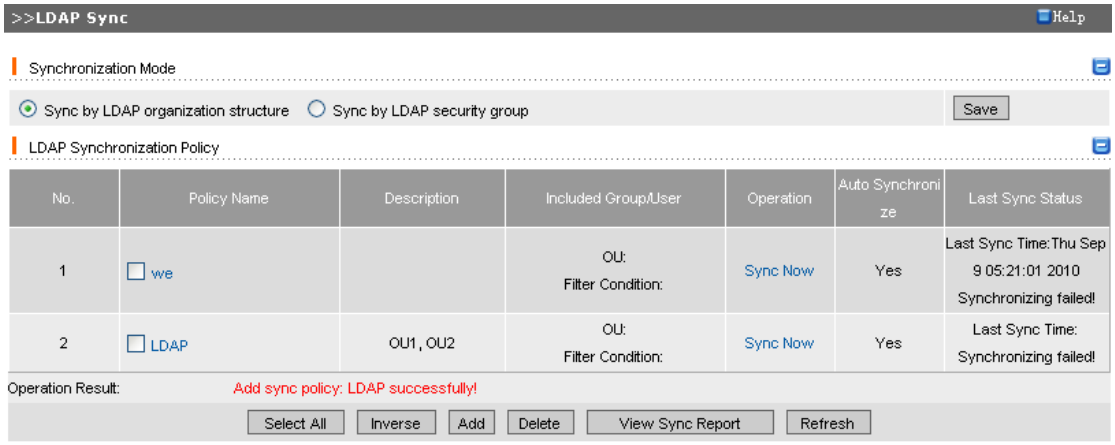
[Filter]: Configures the filtering condition for synchronization, according to the domain parameters. It is blank (with no condition) by default.

[Import From]: Configures the OU starting from where the users and user groups are imported. Options are [Specified OU] and [Sub OU of the specified OU]. [Specified OU] indicates that it imports the users/user groups starting from the configured OU; while [Sub OU of the specified OU] indicates that it imports the user/user groups starting from the sub-OU of the configured OU, its upper hierarchy OU and its users not being imported.

[OU Import Depth]: Configures the depth (maximum hierarchies) of OU being imported; maximum value is 15. In this example, only the ou1 and its sub-OU are imported, the OU below its sub-OU will not be imported; however, the user(s) below the OU will be imported and synchronized to the corresponding user group.

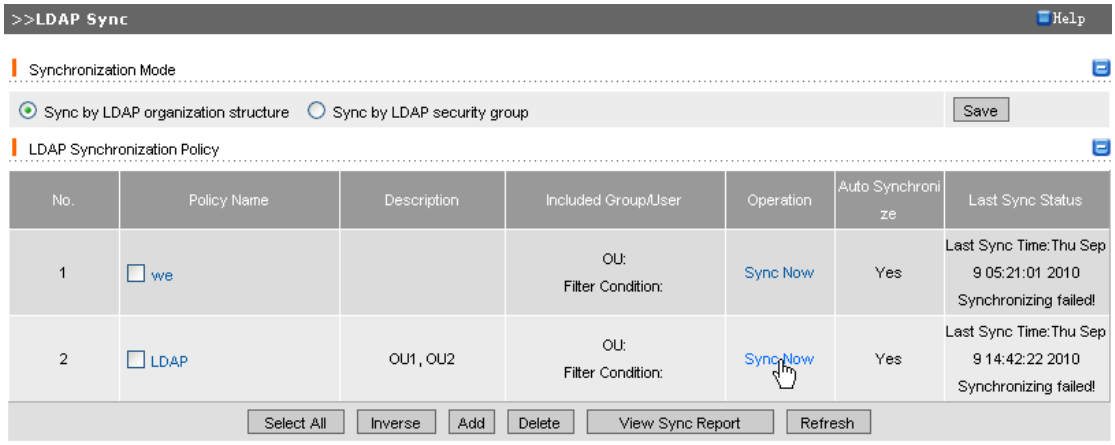
Having completed configuring this synchronization policy, you have to click the <OK> button to save all the settings.

Saving the settings, you will return to the default configuration page. The newly-created synchronization policy is listed, as shown below:



Click <Sync Now> to have the user/user groups synchronized immediately according to the configured synchronization policy.

Click the <Refresh> button to refresh and view the synchronization status, and the [Last Sync Status] is displayed in the list, as shown below:



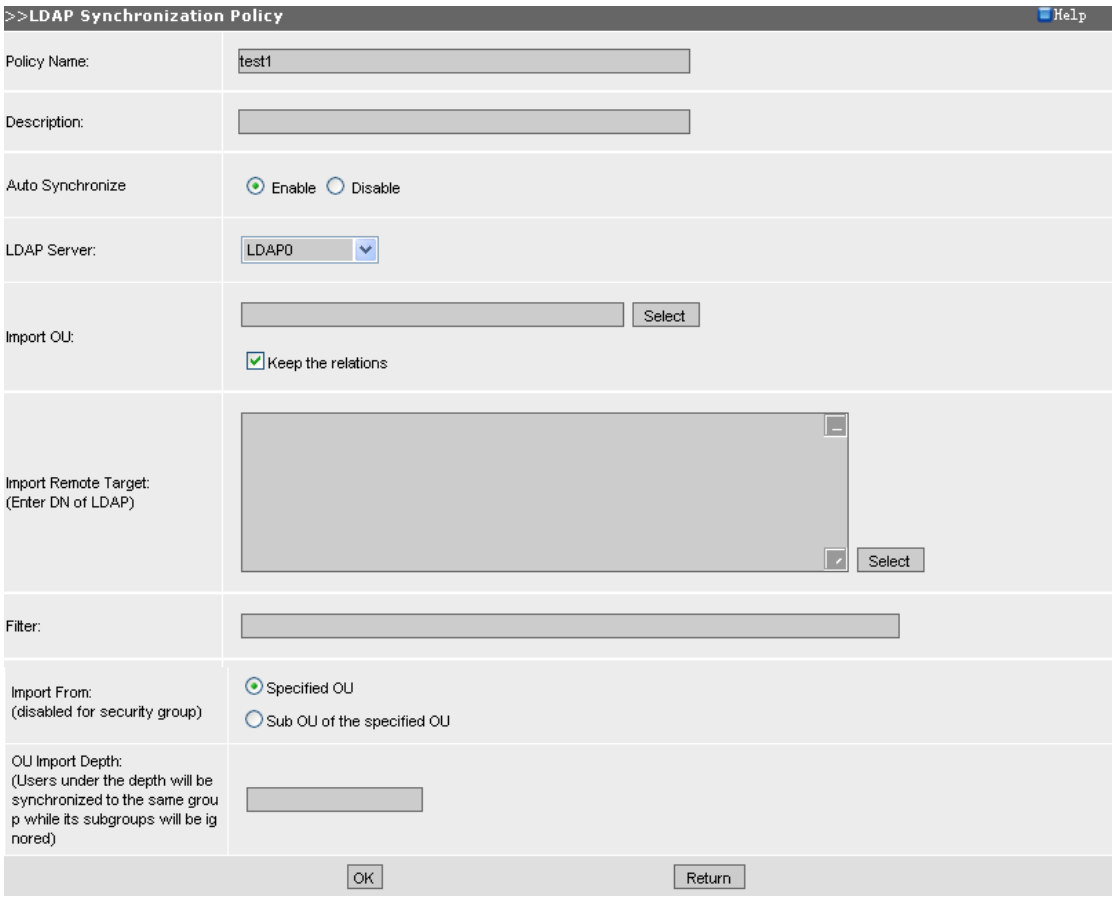
[Last Sync Time]: Displays the time of the latest synchronization and whether it synchronized successfully.

Having imported successfully the organization structure and the users into the IAM gateway device, the group will be seen in the member list.

7.6.2. Sync by LDAP Security Group

[Sync by LDAP security group] synchronization mode imports user/user groups according to the security group.

Select [Sync by LDAP security group], and click the <Add> button and the [LDAP Synchronization Policy] configuration page, as shown below:



The above configurations are nearly the same with those of [Sync by LDAP organization structure], with the only difference that the selected and imported [Import Remote Target] are the security groups of the domain server.

7.6.3. View Sync Report

Each synchronization option of Active Directory will produce its own synchronization report which covers information of group, user name, etc.

Click <View Sync Report> to view all the reports. The page is as shown below:

[Sync Report Name]: Displays the name of the report. Click the report name and you will see the detailed contents of this report.

[Sync Mode]: Displays how the synchronization policy is synchronized, [Sync Now] or [Auto Sync].

[Sync Time]: Displays the time when the synchronization report is generated.

[Sync Status]: Displays whether it is a successful synchronization.

<Clear>: Click this button to clear all the reports recorded.

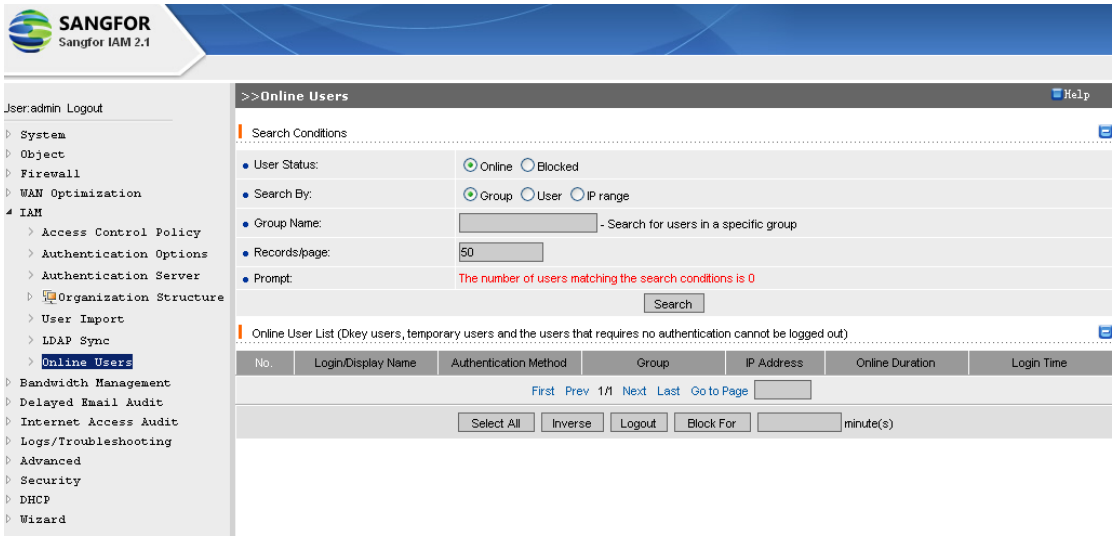
- Each synchronization mode supports maximum 10 synchronization policies.
- Maximum 20 synchronization reports will be saved. If more reports are being generated, the same number of the earliest reports will be deleted. Clicking the <Clear> button can manually delete all the reports.

7.7. Online User

[Online User] enables you to view, search for and manage the online users of the IAM gateway

device.

The configuration page is as shown below:



[Online User List]: Displays the information of the online users that are accessing to the Internet through the IAM gateway device, including information of [No.], [Login/Display Name], [Authentication Method], [Group], [IP Address], [Online Duration] and [Login Time].

<Select All>, <Inverse>: Click it to select the needed user(s).

<Logout>: Click it to force the selected online user(s) to log out.

<Block For>: Click it and configure the time. You can block the selected online user to get online for some time.

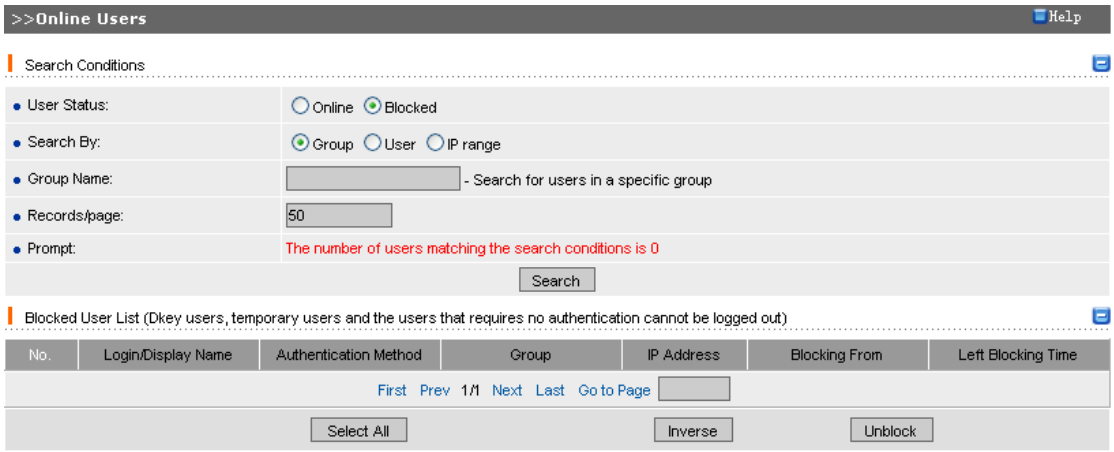
[Search Conditions]: Configures the filtering conditions on searching for user(s).

[Search By]: Select an option according to which the user(s) is searched for. Options are [Group], [User] and [IP range].

[Records/page]: Configures the number of users displayed per page. It is recommended that the displayed records per page be no more than 200.

[User Status]: Configures the status of the user(s) searched for, [Online] or [Blocked].

If the selected [User Status] is [Blocked], the blocked users will be displayed in the [Blocked User List], as shown below:



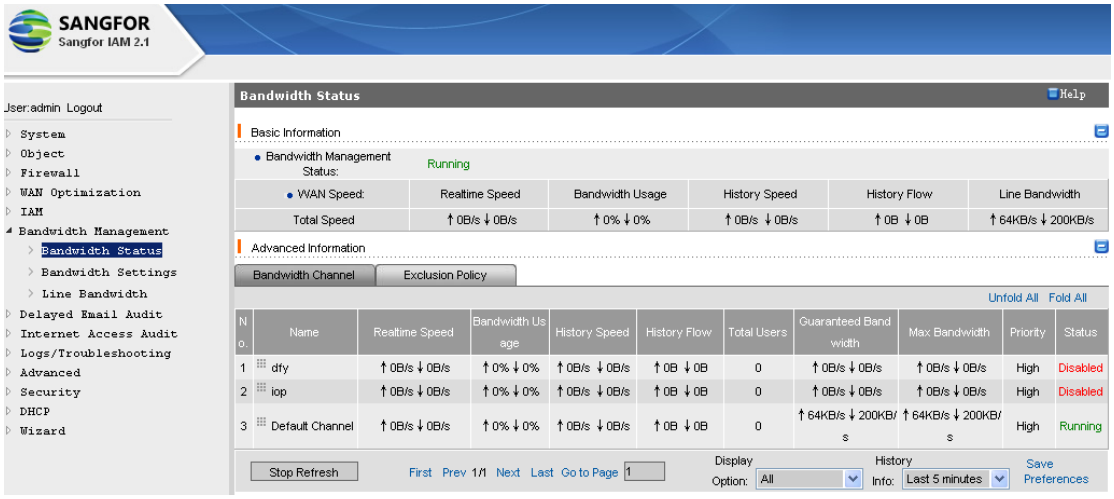
[Blocked User List]: Displays the information of the blocked user(s), including [No.], [Login/Display Name], [Authentication Method], [Group], [IP Address], [Blocking form] and [Left Blocking Time].

<Unblock>: Click this button to unblock the selected blocked user(s). Having been unblocked, the user can then get access to the Internet through the IAM gateway device.

Chapter 8 Bandwidth Management

SANGFOR IAM bandwidth management (BM) module enables you to configure assured bandwidth and bandwidth limitation for the external lines and bandwidth channels. It can guarantee the bandwidth for accessing to some important applications, and limit the uplink/downlink bandwidth as well. Besides, you can create specific policy according to the service, user, guaranteed bandwidth and maximum bandwidth. Sub-channel can also be built for certain bandwidth channel to define the parent channel much finely.

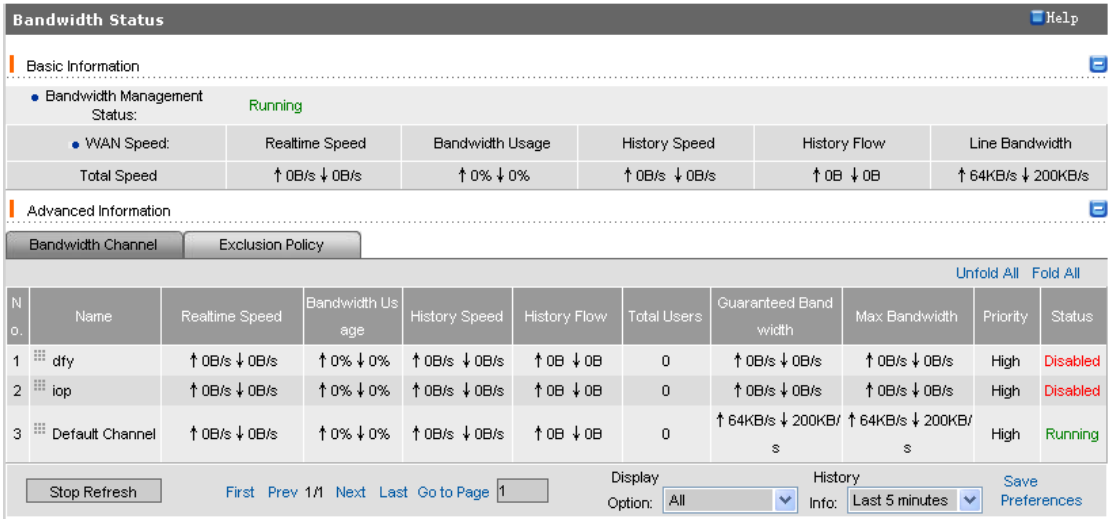
The configuration page is as shown below:



8.1. Bandwidth Status

[Bandwidth Status] covers the status of bandwidth management, flow information of the external lines and bandwidth channel(s).

The page is as shown below:



[Basic Information]: Displays the running status and flow information of the external lines.

<Unfold All>, <Fold All>: Click it to unfold all or fold all the flow information of the channels.

<Stop Refresh>: Click it to stop the function of refreshing the flow information in real time.

[Display Option]: Configures what bandwidth channels are to be displayed. Options are [All] and [Running channels].

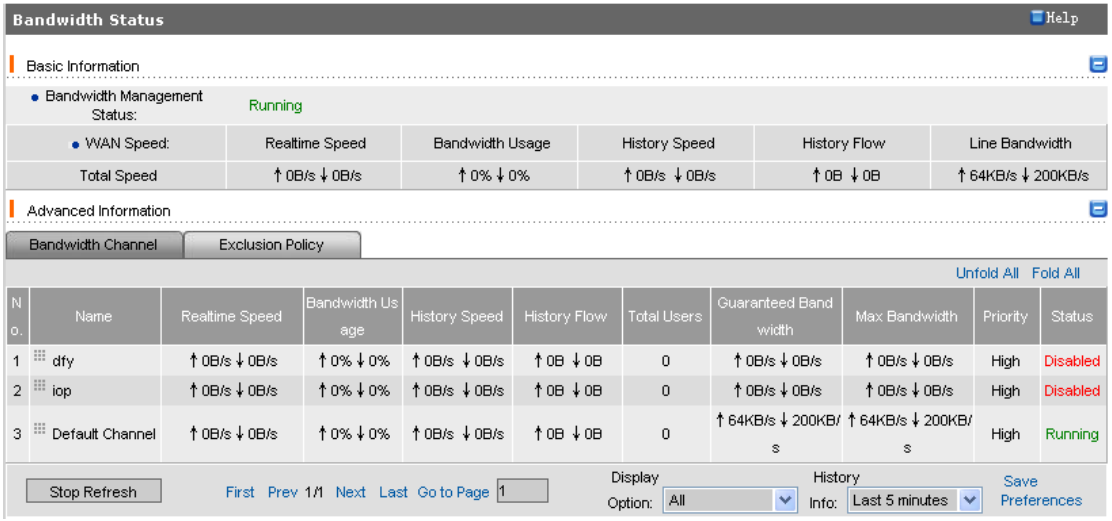
[History Info]: Configures the time period during which the flow and speed statistics are made and displayed in the list.

<Save Preference>: Click it and you will save the [Display Option] and [History Info] configured. This operation will facilitate you to view your preferred statistics (displayed by default) next time.

8.1.1. Bandwidth Channel

[Bandwidth Channel] displays the running status of each bandwidth channel.

The configuration page is as shown below:



[Name]: Displays the name of the channel(s).

[Realtime Speed]: Displays the uplink/downlink bandwidth of the channel in real time.

[Bandwidth Usage]: Displays the percentage of the occupied bandwidth in the total bandwidth.

[History Speed]: Displays the speed calculated according to the history statistics and time.

[History Flow]: Displays the flow calculated according to the history statistics and time.

[Total Users]: Displays the number of users that cause flow of this channel.

[Guaranteed Bandwidth]: Displays the guaranteed bandwidth that the IAM gateway allocates for the channel.

[Max Bandwidth]: Displays the maximum bandwidth configured on the IAM gateway device.

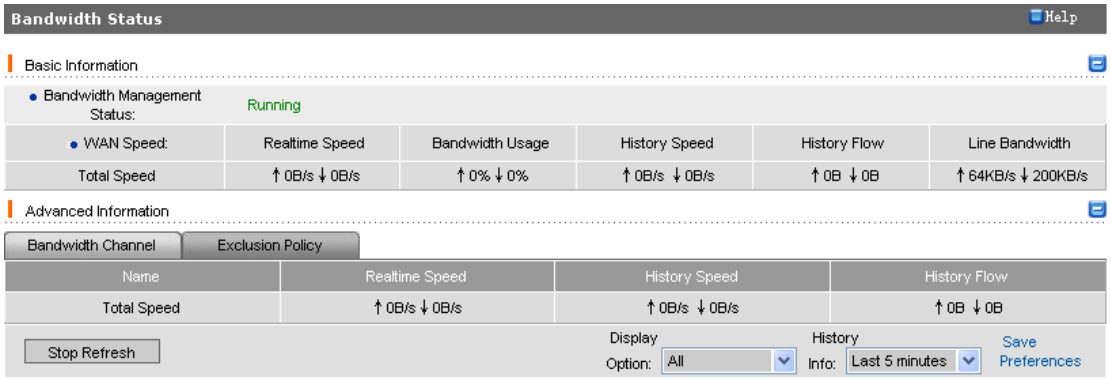
[Priority]: Displays the priority of this channel. The higher priority a channel has, the more extra bandwidth this channel can get.

[Status]: Displays the status of this channel, running, enabled or disabled. If the status of a bandwidth channel is disabled, the bandwidth channel (policy) may get invalid at that time (check the [Schedule] of this policy).

8.1.2. Exclusion Policy

[Exclusion Policy] Displays the realtime speed, history speed and history flow of the applications that are not involved in the bandwidth channels (policies).

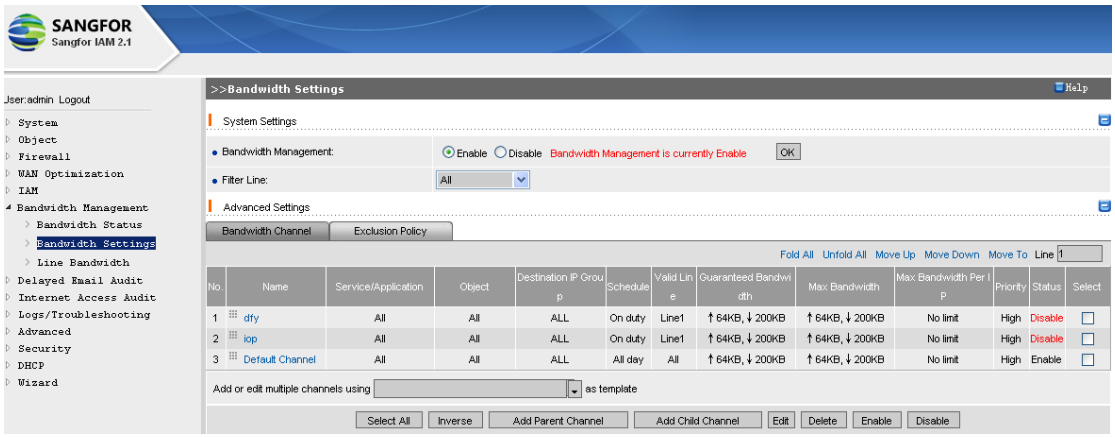
The page is as shown below:



8.2. Bandwidth Settings

[Bandwidth Settings] configures the bandwidth allocation for each line.

The configuration page is as shown below:



[Bandwidth Management]: Select [Enable] and click the <OK> button to activate the bandwidth management function.

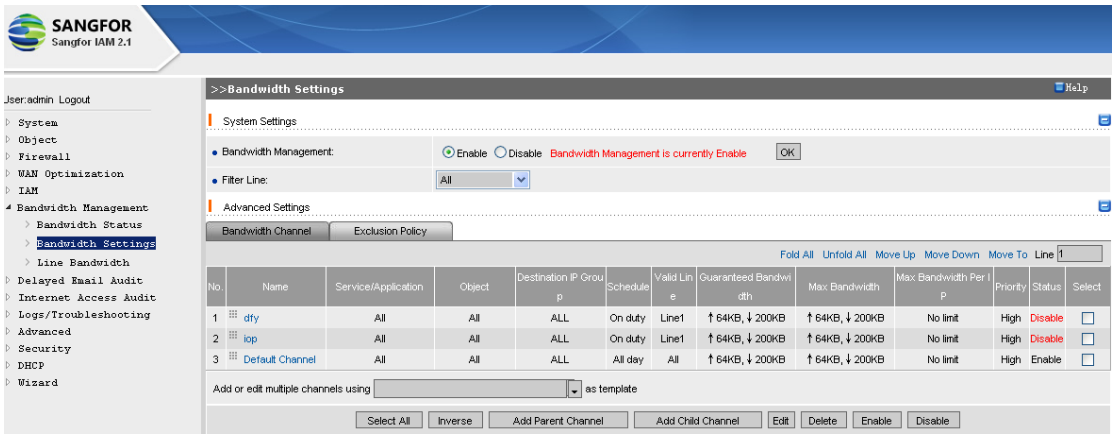
[Filter Line]: Select an option to have the corresponding bandwidth channel (s) displayed in the bandwidth channel list.

8.2.1. Bandwidth Channel

SANGFOR IAM bandwidth management (BM) module offers bandwidth allocation function to configure assured bandwidth and bandwidth limitation.

You can define a bandwidth channel according to the service and application, object, schedule, external line, destination IP group, to achieve both assuring bandwidth and limiting bandwidth, and can build sub-channel for certain bandwidth channel to define the parent channel in detail.

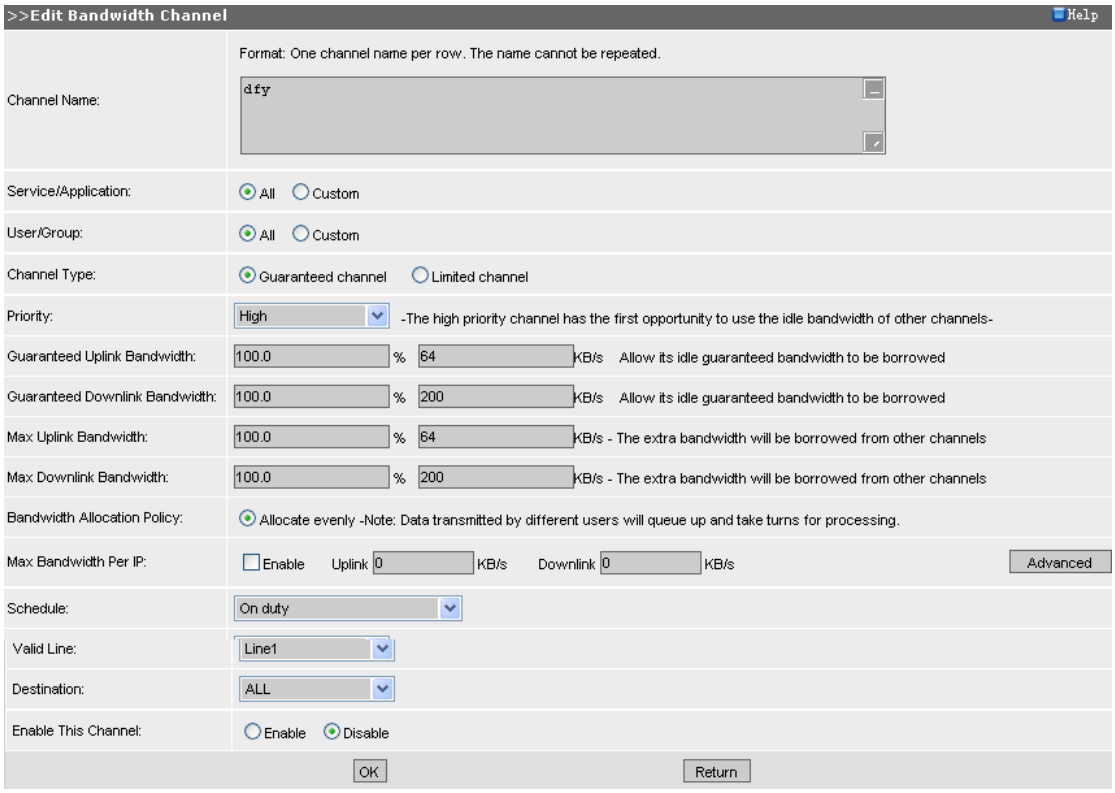
The page is as shown below:



The bandwidth channel policies are matched from top to bottom.

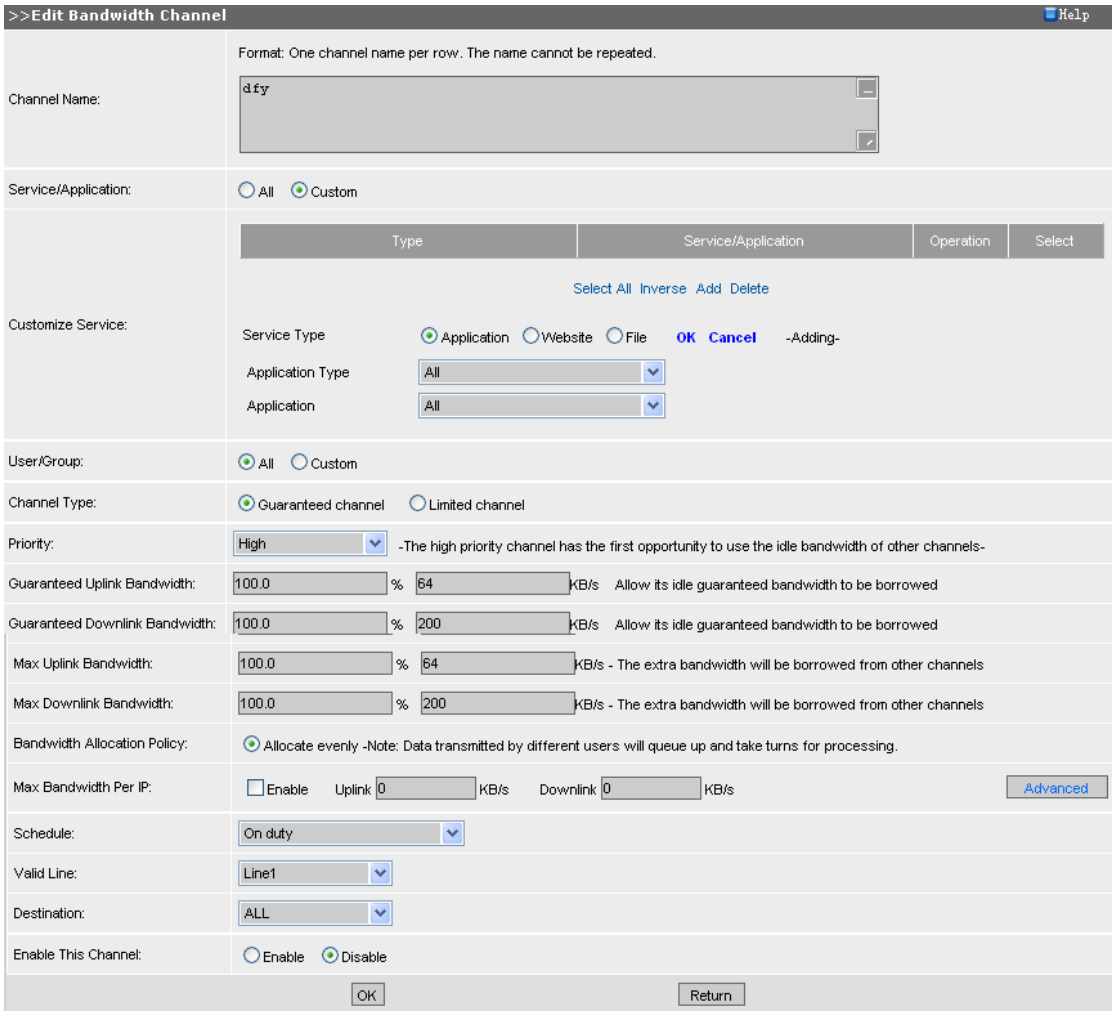
8.2.1.1. Add Bandwidth Channel

Click the <Add Parent Channel> button, and the [Edit Bandwidth Channel] configuration page appear, as shown below:



[Channel Name]: Type one more names for the bandwidth channel(s). One name per row, length of each name is within 96 characters.

[Service/Application]: Configured the specific service(s) applied to this bandwidth channel. If [Custom] is selected, you can define and add services. Click <Add> and the corresponding options appear, as shown below:



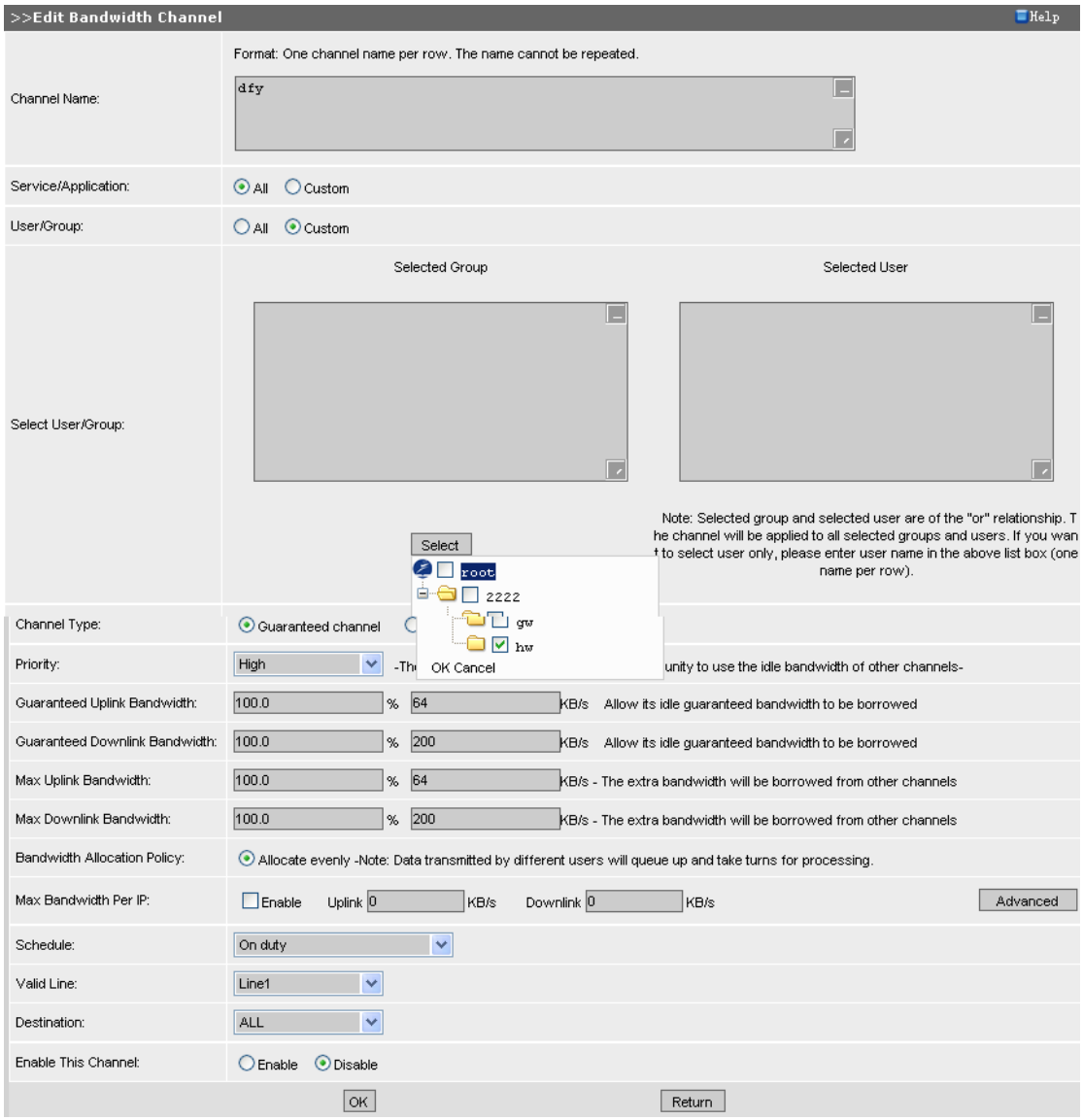
[Service Type]: Options are [Application], [Website] and [File].

If [Application] is selected, you need then select an [Application Type] and a specific [Application].

If [Website] is selected, you need then select a [Website Type] from the internal library.

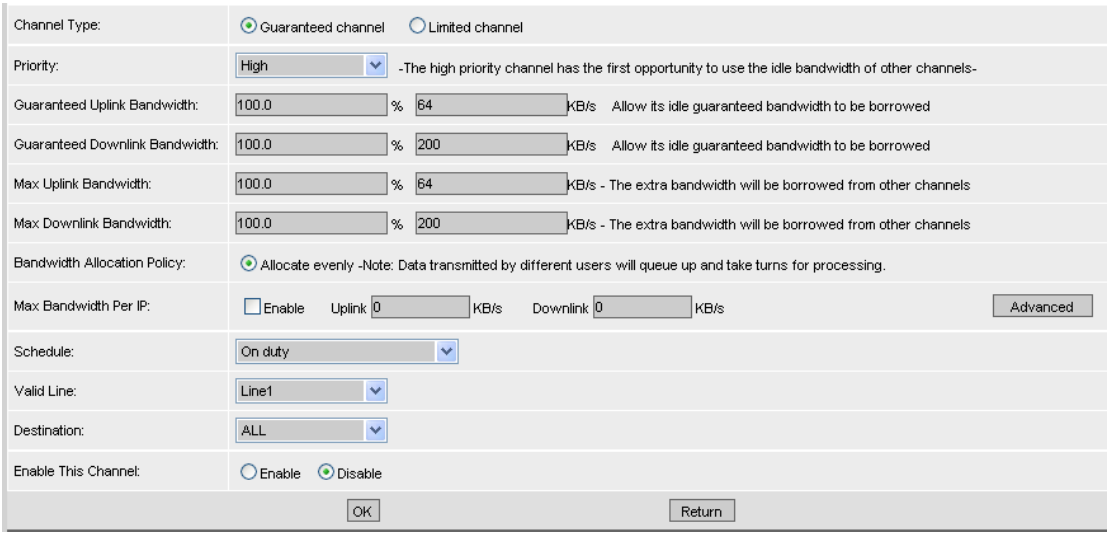
If [File] is selected, you need then select a [File Type] from the file type group.

[User/Group]: Configures the valid users and user groups. You can select [All] to have all the user and user groups applied to this policy, or select [Custom] to have some of the users or user groups be applied to this policy. The configuration page is as shown below:



[Channel Type]: Defined the type of the bandwidth channel, [Guaranteed channel] or [Limited channel]. If the selected one is [Guaranteed channel], this policy will guarantee the user with the minimum bandwidth; if the selected one is [Limited channel], this policy will limit the bandwidth for the services available online.

Select [Guaranteed channel] and the following items appear, as shown below:

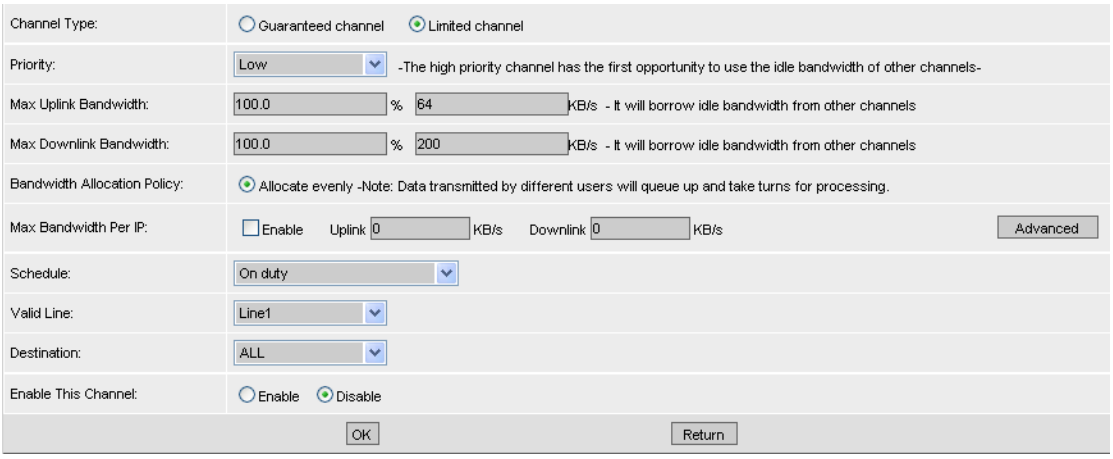


[Priority]: Options are [High], [Medium] and [Low]. The bandwidth channel with higher priority is preferred to be assigned with idle bandwidth (from other bandwidth channels).

[Guaranteed Uplink], [Guaranteed Downlink Bandwidth]: Configures the bandwidth or percentage of the guaranteed uplink/downlink bandwidth in the total bandwidth allocated.

[Max Uplink Bandwidth], [Max Downlink Bandwidth]: Configures the upper limit of uplink/downlink bandwidth width or rate of this bandwidth channel.

Or select [Limited channel] and the following items appear, as shown below:



[Bandwidth Allocation Policy]: Configures the bandwidth for the users and the specific service/application that applies to this bandwidth chancel (policy).

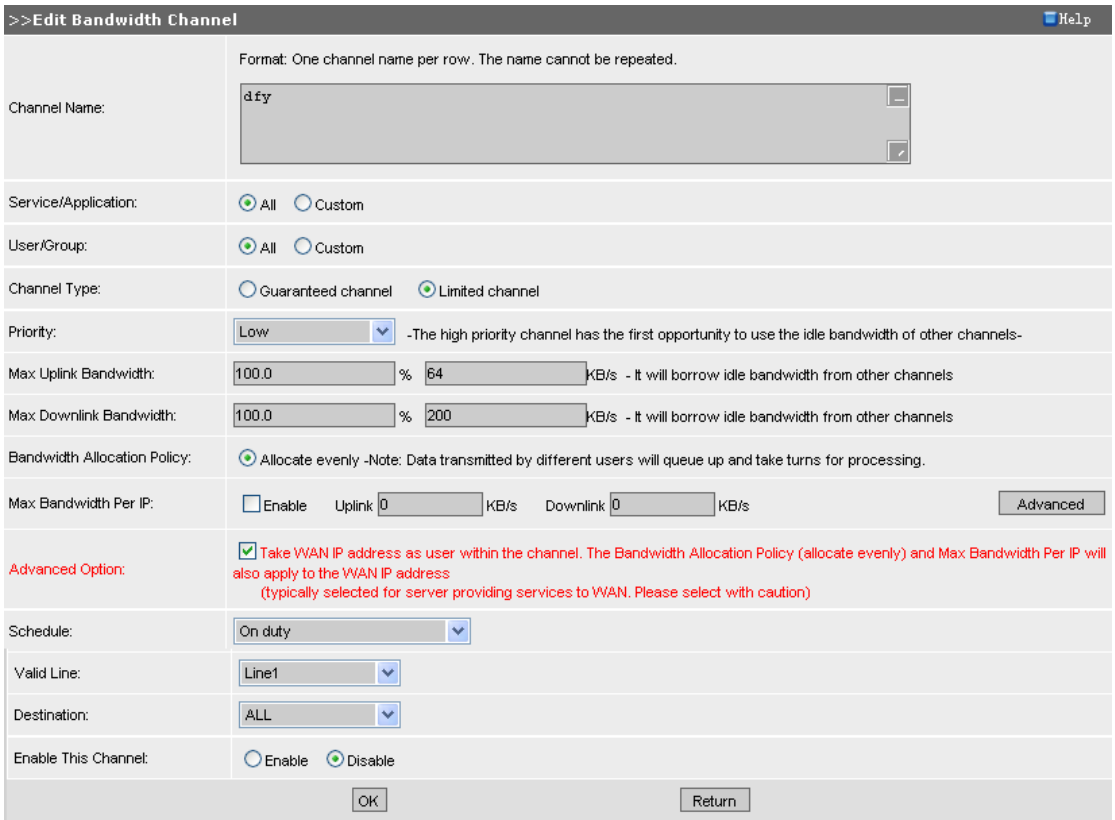
[Allocate evenly]: Indicates that if there are 20 online users with [Guaranteed uplink bandwidth] 40KB/S, each of the user will be ensured with at least 2KB/S uplink bandwidth.

[Max Bandwidth Per IP]: Click [Enable] and configure the [Uplink] and [Downlink] to limit the maximum uplink/downlink bandwidth of a single user (IP address) respectively.

[Max Bandwidth Per IP] is configured with a bandwidth value instead of a rate, and free from the impact of other bandwidth settings; while [Guaranteed Uplink/Downlink Bandwidth] and [Max Uplink/Downlink Bandwidth] are configured with a rate, which indicates that the actual bandwidth varies from the total bandwidth settings for this channel.

[Advanced]: Check this option to open the [Advanced Option] page. If you check the advanced option, the external IP address (node) will be taken as one member of the LAN users (nodes), that is to say, the [Allocation Policy] and [Max Bandwidth Per IP] will also be applied to the external IP address(es), which will lower down the performance of the IAM gateway if there are lots of external nodes.

The configurations are as shown below (in red):



[Schedule]: Configures the time period during which this bandwidth channel (policy) will get valid.

[Valid Line]: Configures the external line to which this bandwidth channel (policy) applies.

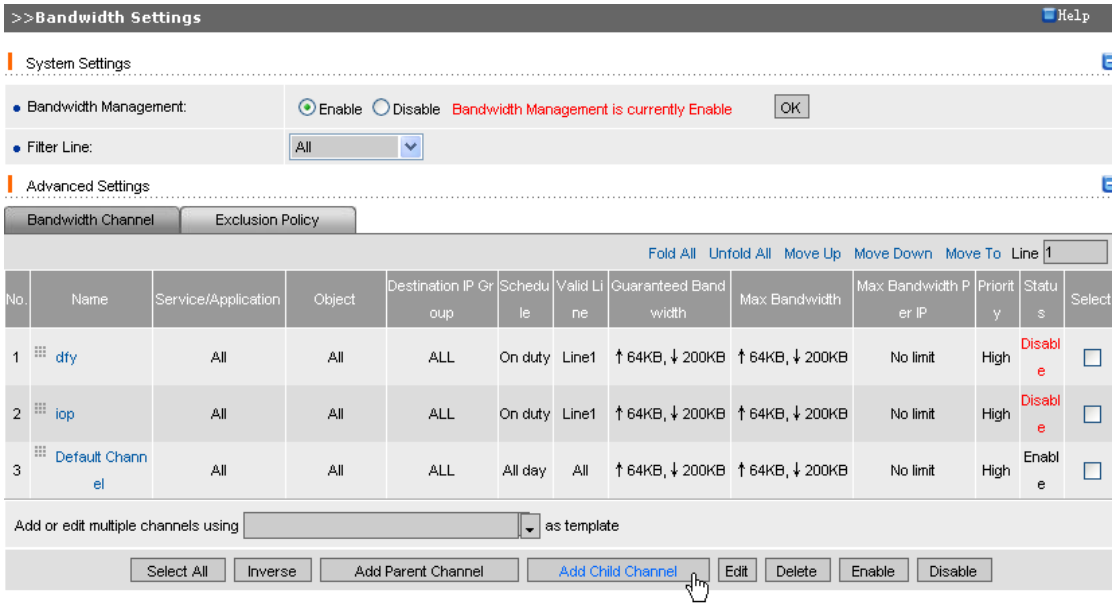
[Destination]: Configures the destination IP address to which this bandwidth channel (policy) applies.

[Enable This Channel]: Select [Enable] or [Disable] to have this bandwidth policy get valid or invalid respectively.

8.2.1.2. Add Child Bandwidth Channel

SANGFOR IAM gateway allows you to further define an existing bandwidth channel, and to divide the bandwidth of it much finely.

Under the [Bandwidth Settings] configuration page, select an existing bandwidth channel, and then click the <Add Child Channel> button to enter the [Edit Bandwidth Channel] to add a sub-channel.



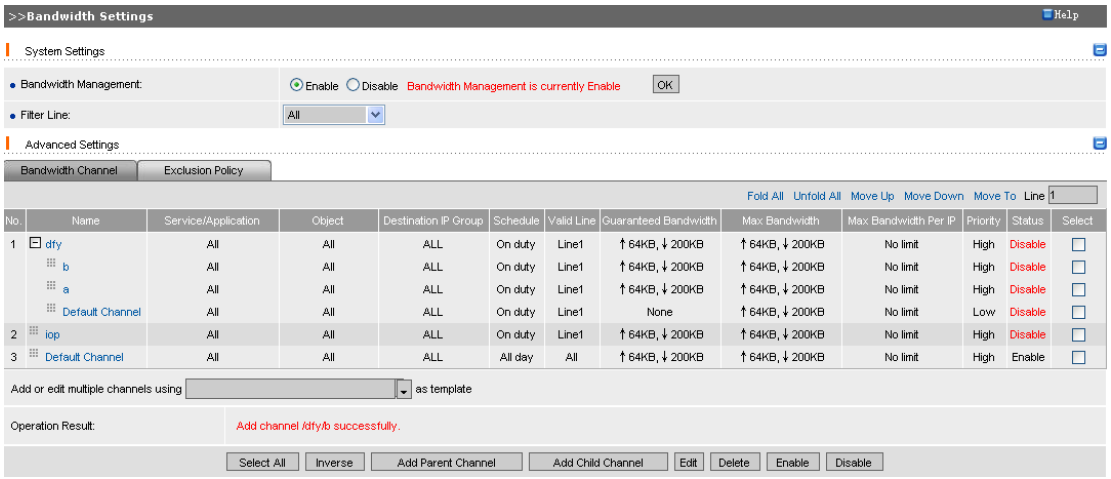
- The rate configured and bandwidth calculated and allocated for the sub-channel (child channel) are based on its parent channel; the total bandwidth will never exceed that of its parent channel.
- The BM module of IAM gateway device supports maximum three hierarchies. Each parent channel has an internal default channel which cannot be deleted. This default channel is used for other flow to which none of the other bandwidth channels (policies) is applied.
- The configuration of a child channel is nearly the same with that of its parent channel. For detailed introductions, please refer to the above section, Section 8.2.1.1 Add Bandwidth

Channel.

8.2.1.3. Select and Edit Bandwidth Channel

Under the [Bandwidth Settings] configuration page, click <Select All> to select all the existing bandwidth channels, or click <Inverse> to only select the currently unselected bandwidth channels.

The configuration page is as shown below:



[Name]: Click the name of a bandwidth channel to get into the [Edit Bandwidth Channel] page and edit this bandwidth channel (policy).

<Enable>, <Disable>, <Delete>: Select one or more bandwidth channels, and then click <Enable>, <Disable> or <Delete> button to enable, disable or delete the bandwidth channel (policy) respectively.

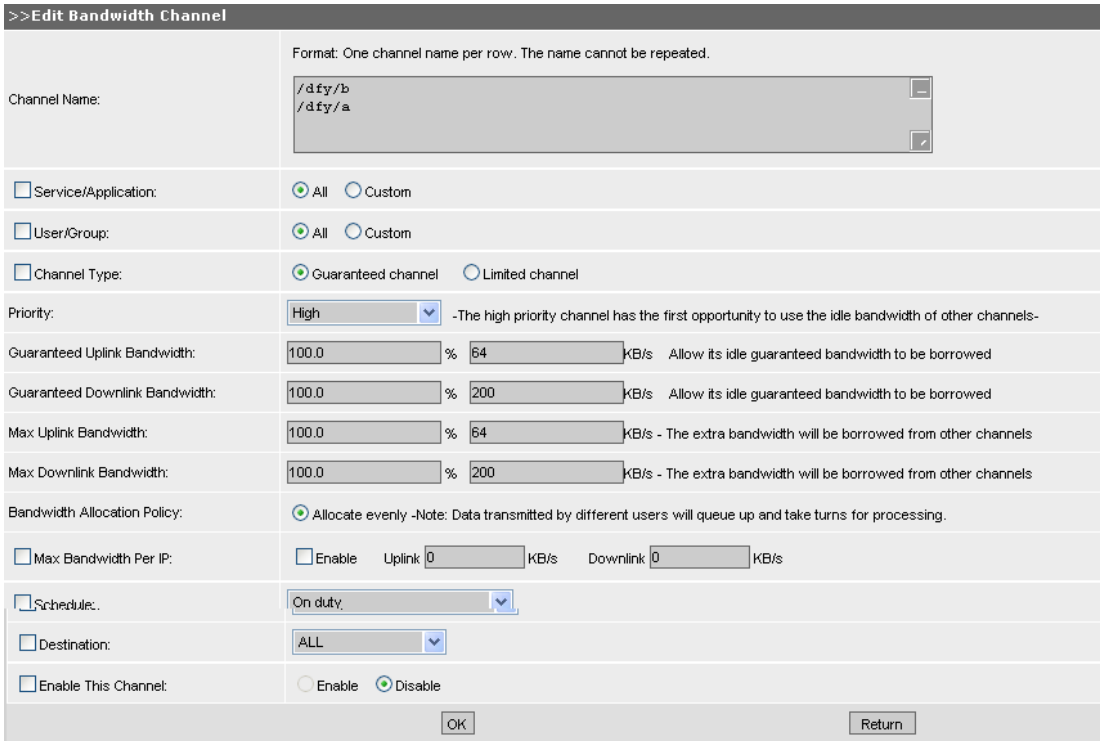
<Unfold All>, <Fold All>: Click it to view (unfold) or fold the information of all the bandwidth channels.

<Move Up>, <Move Down>, <Move To>: Click <Move Up>, <Move Down> to move the selected bandwidth channel up or down respectively; or click the <Move To> and type a line number to move the selected bandwidth channel to an specified place (row).

- The [Default Channel] in the [Bandwidth Channel] list is the system default channel, and cannot be deleted.
- The bandwidth channels are matched according to the features of the flow, from top to bottom.

To edit multiple bandwidth channels at the same time, you have to first select the needed bandwidth channels and then select a template.

Click the <Edit> button, and the configuration page pops up, as shown below:



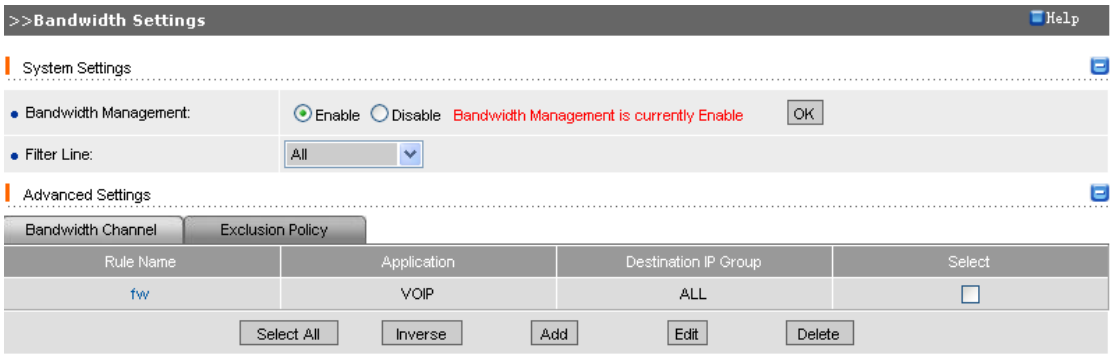
- [Service/Application], [User/Group], [Channel Type], [Max Bandwidth Per IP], [Schedule], [Valid Line], [Destination], [Enable This Channel] configurations are the same with those introduced above.

- [Bandwidth Type] and [Valid Line] must be checked or unchecked at the same time.

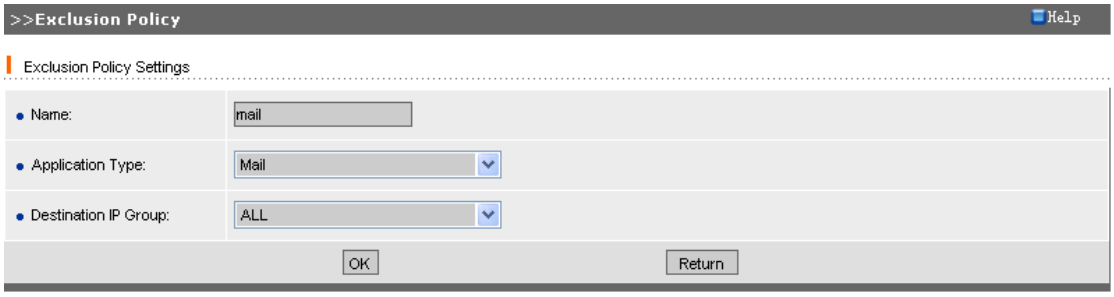
8.2.2. Exclusion Policy

[Exclusion Policy] functions while the local area network has a proxy which is deployed at the WAN interface end of the SANGFOR IAM gateway device. The exclusion policy will free the LAN users from limitations such as guaranteed bandwidth and maximum bandwidth.

The configuration page is as shown below:



Click the <Add> button to enter the [Exclusion Policy] configuration page and add a new exclusion policy, as shown below:



[Name]: Type a name for this exclusion policy.

[Application Type]: Select an application type that will not be limited by guaranteed uplink/downlink bandwidth or maximum uplink/downlink bandwidth.

[Destination IP Group]: Select the IP address of the to-be-accessed server.

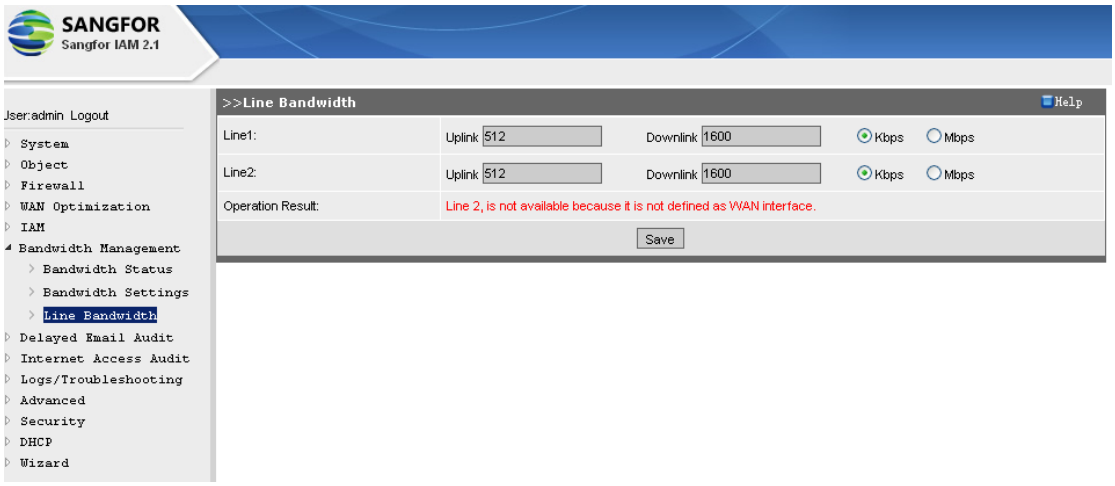
Please DO think it over to add an exclusion policy, for the exclusion policy will ignore the bandwidth settings. In that case, all the matching traffic will be free from the control of the

bandwidth management module, that is to say, the physical bandwidth may be used out, which may result in congestion of the lines.

8.3. Line Bandwidth

[Line Bandwidth] configures the actual uplink and downlink bandwidth of the external line(s). It is the base of [Guaranteed Bandwidth] and [Limited Bandwidth] configuration.

The configuration page is as shown below:



- Bandwidth configuration can be in unit of Kbps and Mbps.
- Under the Bridge mode, the virtual line will be automatically enabled. Maximum 4 virtual lines can be configured on each IAM gateway device.
- Inappropriate line bandwidth settings will lead to waste of bandwidth (the value is lower than need), or lead to congestion (the value is higher than need).

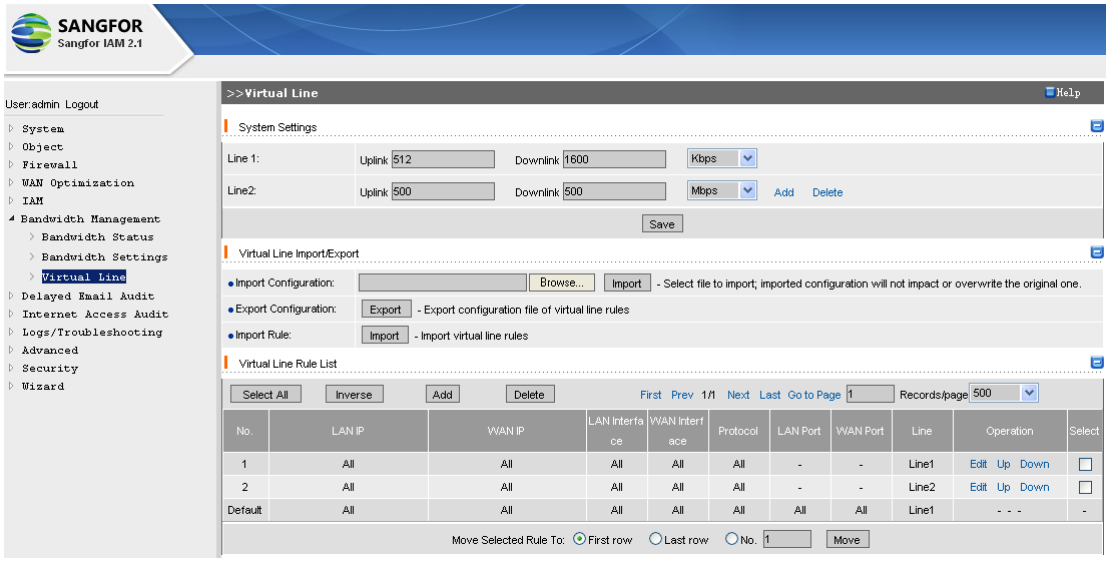
8.4. Virtual Line

[Virtual Line] configures the multiple virtual lines for a physical line. It is only available for

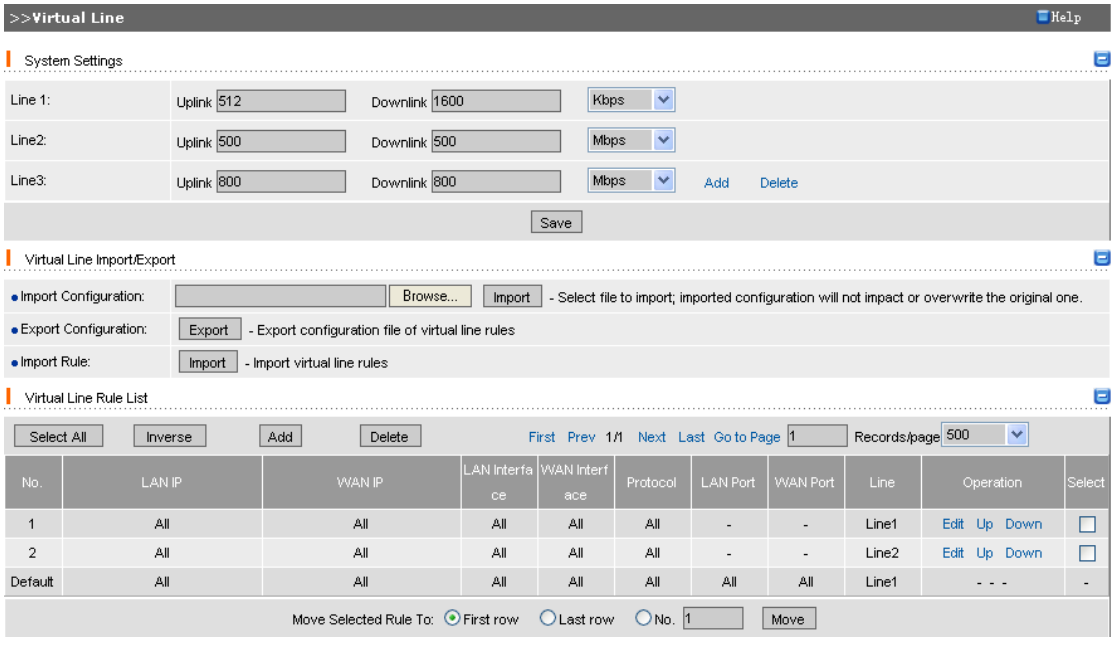
Bridge-mode deployment.

[System Settings]: Configures the uplink/downlink bandwidth of the virtual lines. Idle bandwidth of a virtual line cannot be borrowed by another virtual line, and the total bandwidth of the all the virtual lines must NOT be more than the total bandwidth of the physical line. One IAM gateway device supports maximum 4 virtual lines.

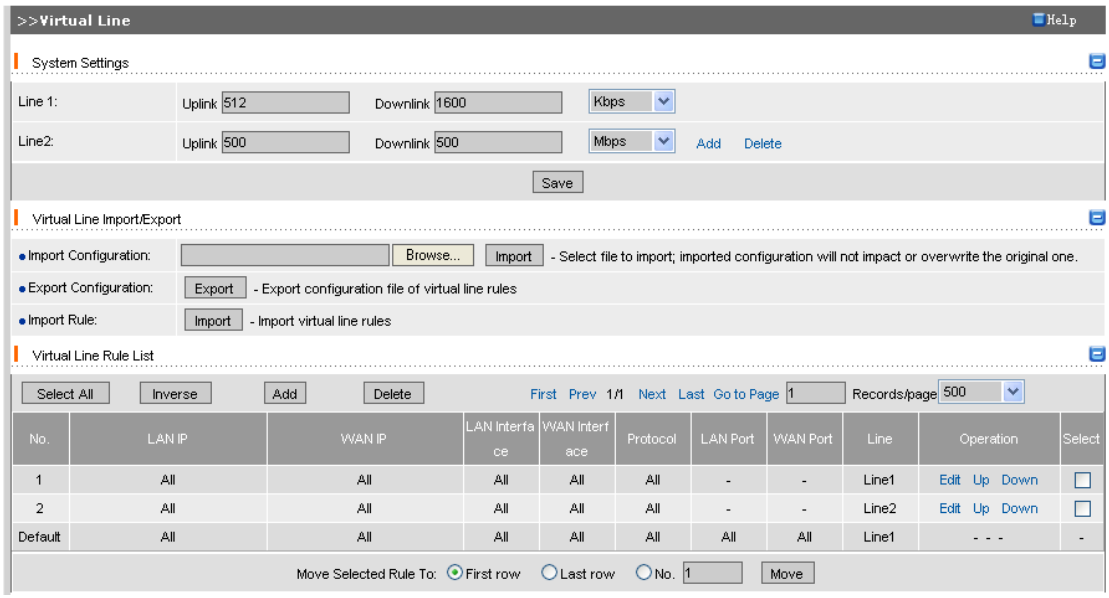
The configuration page is as shown below:


SANGFOR
Sangfor IAM 2.1
User:admin Logout
System
Object
Firewall
WAN Optimization
IAM
Bandwidth Management
Bandwidth Status
Bandwidth Settings
Virtual Line
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Security
Wizard
>>Virtual Line
Help
System Settings
Line 1: Uplink 512 Downlink 1600 Kbps
Line2: Uplink 500 Downlink 500 Mbps Add Delete
Save
Virtual Line Import/Export
Import Configuration: Browse... Import - Select file to import; imported configuration will not impact or overwrite the original one.
Export Configuration: Export - Export configuration file of virtual line rules
Import Rule: Import - Import virtual line rules
Virtual Line Rule List
Select All Inverse Add Delete First Prev 1/1 Next Last Go to Page 1 Records/page 500
No. LAN IP WAN IP LAN Interface WAN Interface Protocol LAN Port WAN Port Line Operation Select
1 All All All All All - - Line1 Edit Up Down
2 All All All All All - - Line2 Edit Up Down
Default All All All All All All All Line1 - - -
Move Selected Rule To: First row Last row No. 1 Move

Click the <Add> to create a new line; configure this line and then click the <Save> button, as shown below:


>>Virtual Line
Help
System Settings
Line 1: Uplink 512 Downlink 1600 Kbps
Line2: Uplink 500 Downlink 500 Mbps
Line3: Uplink 800 Downlink 800 Mbps Add Delete
Save
Virtual Line Import/Export
Import Configuration: Browse... Import - Select file to import; imported configuration will not impact or overwrite the original one.
Export Configuration: Export - Export configuration file of virtual line rules
Import Rule: Import - Import virtual line rules
Virtual Line Rule List
Select All Inverse Add Delete First Prev 1/1 Next Last Go to Page 1 Records/page 500
No. LAN IP WAN IP LAN Interface WAN Interface Protocol LAN Port WAN Port Line Operation Select
1 All All All All All - - Line1 Edit Up Down
2 All All All All All - - Line2 Edit Up Down
Default All All All All All All All Line1 - - -
Move Selected Rule To: First row Last row No. 1 Move

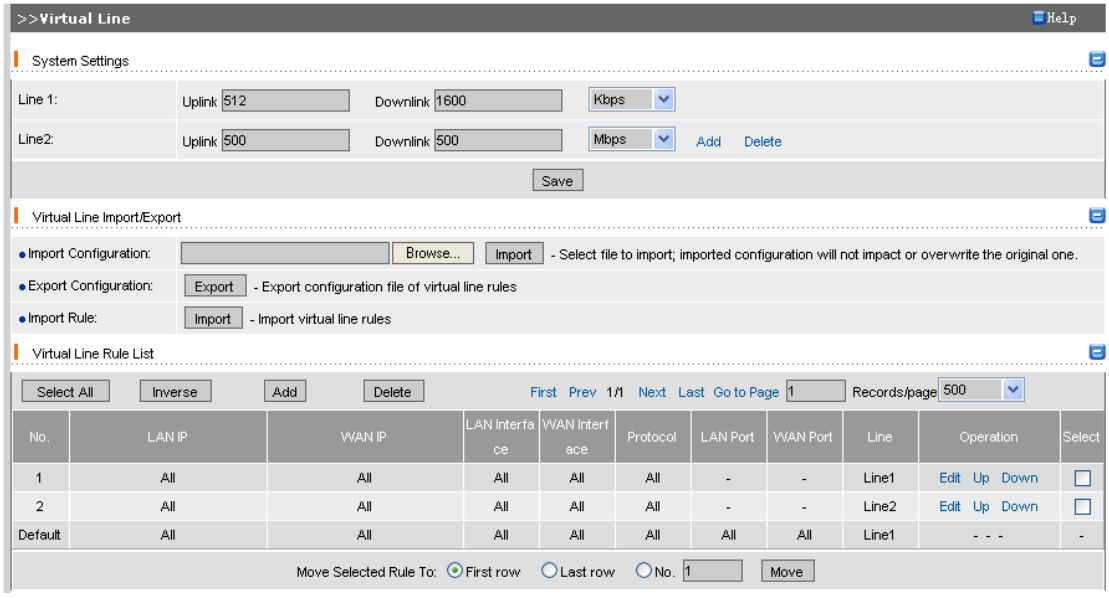
Click <Delete> and then click <Save> button to delete the line, as shown below:


>>Virtual Line
Help
System Settings
Line 1:
Uplink 512
Downlink 1600
Kbps
Line2:
Uplink 500
Downlink 500
Mbps
Add
Delete
Save
Virtual Line Import/Export
Import Configuration:
Browse...
Import
- Select file to import; imported configuration will not impact or overwrite the original one.
Export Configuration:
Export
- Export configuration file of virtual line rules
Import Rule:
Import
- Import virtual line rules
Virtual Line Rule List
Select All
Inverse
Add
Delete
First Prev 1/1 Next Last Go to Page 1 Records/page 500
No. LAN IP WAN IP LAN Interface WAN Interface Protocol LAN Port WAN Port Line Operation Select
1 All All All All All - - Line1 Edit Up Down
2 All All All All All - - Line2 Edit Up Down
Default All All All All All All All Line1 - - -
Move Selected Rule To: First row Last row No. 1 Move

SANGFOR IAM gateway device enables you to create a [Virtual Line Rule List]. It functions when there are multiple external lines connecting to the front-end Internet device (of the IAM gateway device) or there are several Internet devices connecting to the front end of the IAM gateway device, and the gateway mode of the IAM gateway device is Bridge mode [Multi-Bridge].

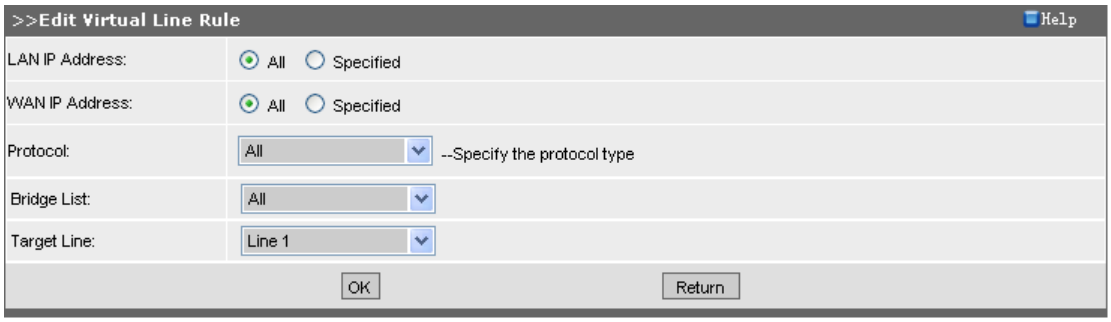
Configure the virtual line rule(s) according to certain policy (configuring external/internal network IP address and port, protocol, etc.), so as to forward the specific data to the assigned bridge, and therefore, to more efficiently control and make full use of the bandwidth.

The [Virtual Line Rule List] is as shown below:


>>Virtual Line
Help
System Settings
Line 1:
Uplink 512
Downlink 1600
Kbps
Line2:
Uplink 500
Downlink 500
Mbps
Add
Delete
Save
Virtual Line Import/Export
Import Configuration:
Browse...
Import
- Select file to import; imported configuration will not impact or overwrite the original one.
Export Configuration:
Export
- Export configuration file of virtual line rules
Import Rule:
Import
- Import virtual line rules
Virtual Line Rule List
Select All
Inverse
Add
Delete
First Prev 1/1 Next Last Go to Page 1 Records/page 500
No. LAN IP WAN IP LAN Interface WAN Interface Protocol LAN Port WAN Port Line Operation Select
1 All All All All All - - Line1 Edit Up Down
2 All All All All All - - Line2 Edit Up Down
Default All All All All All All All Line1 - - -
Move Selected Rule To: First row Last row No. 1 Move

<Up>, <Down>: Click the button to adjust the priority of each virtual line rule. You can also select a rule and then select [First row] or [Last row] to move the selected the rule to top or bottom, or select [No.] to move the selected virtual line to a specified row. As to the rules of the same type, the upper one(s) has higher priority to be matched.

Click the <Add> button to enter the [Edit Virtual Line Rule] configuration page, as shown below:



[LAN IP Address], [WAN IP Address]: Configures respectively the LAN IP and WAN IP from which the data packets are to be matched by the virtual line rule. The IP can be [All] the IP addresses or the [Specified] IP addresses.

[Protocol]: Select the protocol for packet transmission; options are [All], [TCP], [UDP], [ICMP] and [Others]. Select [TCP] or [UDP], and then you have to configure [LAN Port] and [WAN Port]; select [Others] and you have to configure [Protocol Number].

[LAN Port], [WAN Port]: Configures respectively the LAN port and WAN port through which the data packets are transmitted.

[Target Line]: Configures the line that acts as the egress to forward the data packets to the external networks. The data packets will be forwarded to the external network through this line when the conditions configured above are satisfied.

- As to the configuration of uplink/downlink bandwidth of a line, you can choose either Kbps or Mbps as the unit.
- The virtual line rule must be coherent to the link selection policy configured on the front-end device. Generally, you can import the policy-routing table of the front-end device.
- A bridge can have several virtual lines and multiple bridges may belong to a same virtual line.

- Maximum 4 virtual lines are supported by one IAM gateway device.
- [Virtual Line] configuration is only available for Bridge mode.

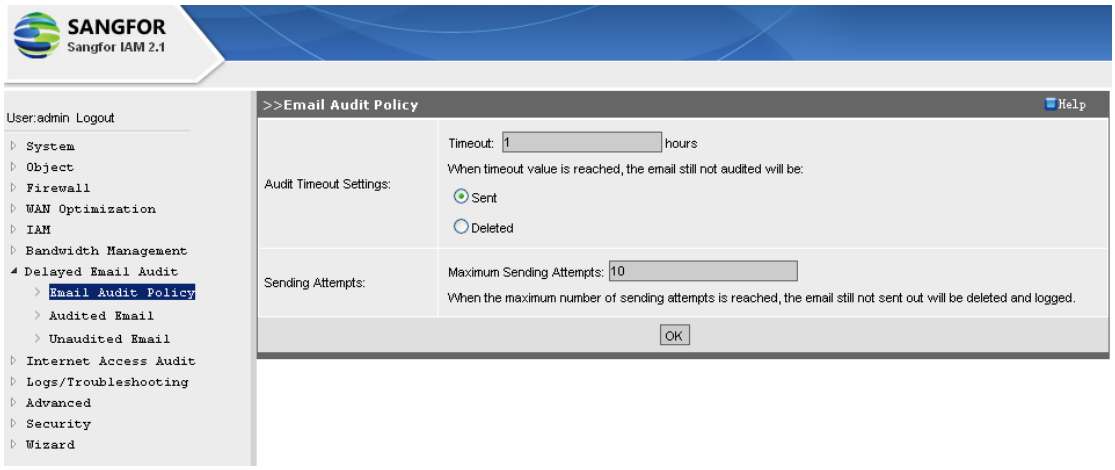
Chapter 9 Delayed Email Audit

[Delayed Email Audit] configures the options for auditing some specific emails, including [Email Audit Policy], [Audited Email] and [Unaudited Email].

9.1. Email Audit Policy

[Email Audit Policy] defines the email audit policy to handle the applicable emails. Configurations are [Audit Timeout Settings] and [Sending Attempts].

Click [Delayed Email Audit] or [Email Audit Policy], the [Edit Audit Policy] configuration page appears, as shown below:

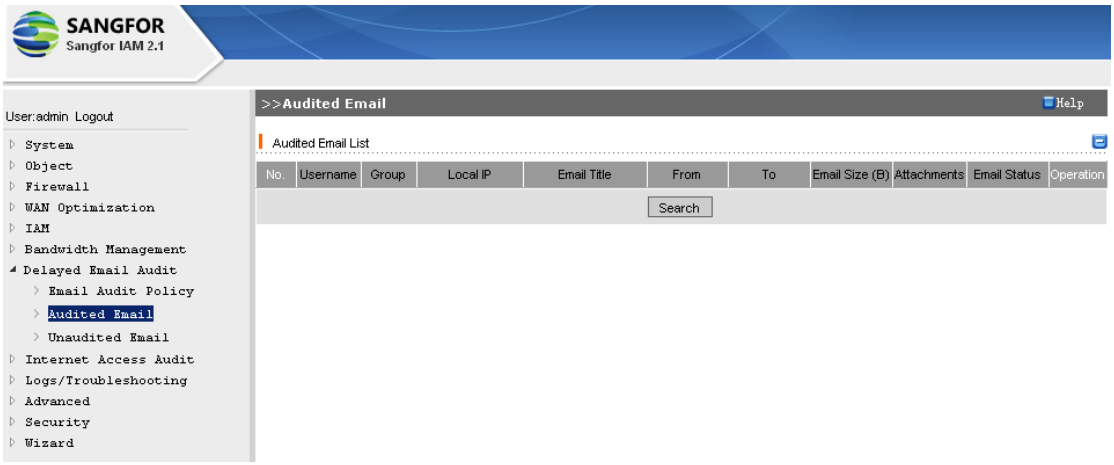


[Timeout:]: Configures the timeout for audit. It is 1 hour by default.

[When timeout value is reached, the email still not audited will be]: Configures the handling method to the unaudited email if the audit timeout is reached, [Sent] or [Deleted] (from the disk).

[Maximum Sending Attempts]: Configures the maximum attempts the email is sent. If the number of tries reaches the maximum attempts, the to-be-sent email will be deleted.

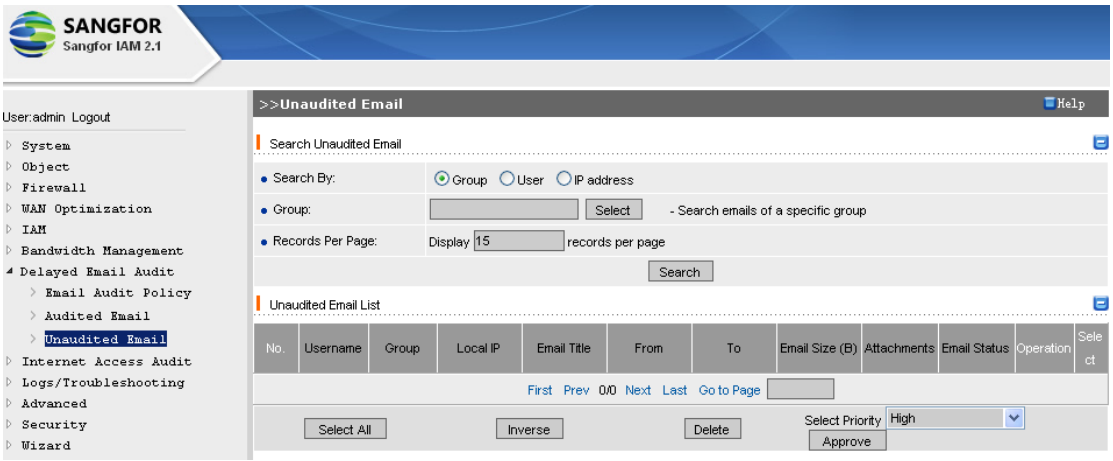
9.2. Audited Email



All the already audited emails or the to-be-sent emails will be listed here, as shown in the above figure.

The audited emails can be searched for in the Data Center of the IAM gateway device (click [Internet Access Audit] > [Enter Data Center] to get into the internal Data Center).

9.3. Unaudited Email



[Search By]: Select an object, [Group], [User] or [IP address].

Then click the <Search> button to have the matching unaudited emails listed. Click <Download> to view the contents of the corresponding email.

<Select All>, <Inverse>: Click it to select the needed email(s).

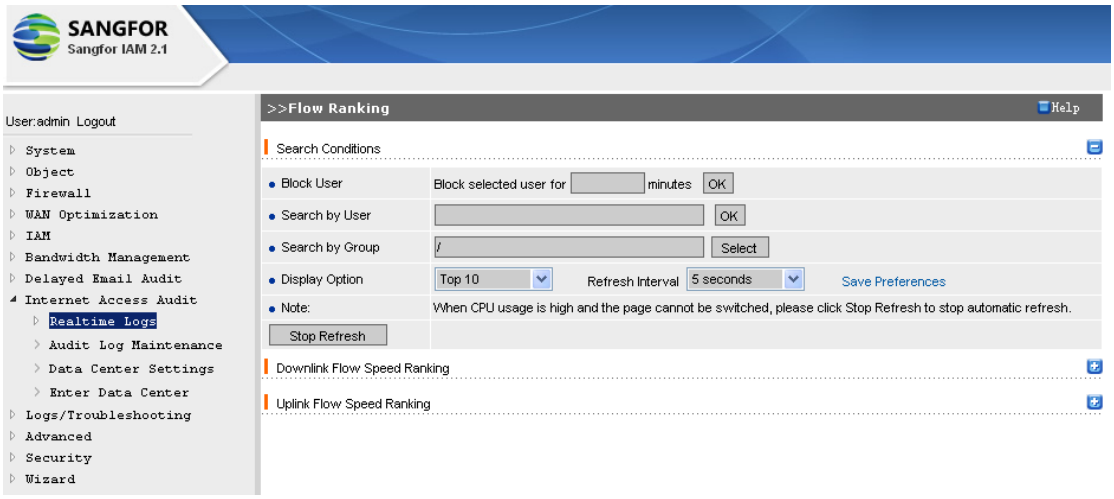
Having audited a selected email, click the <Approve> button to have the selected email get passed; or click <Delete> button to delete the selected email(s).

<Select Priority>: Select a priority to define the audited and selected emails.

Chapter 10 Internet Access Audit

[Internet Access Audit] covers [Realtime Logs], [Audit Log Maintenance], [Data Center Settings] and [Enter Data Center].

The default configuration page of [Internet Access Audit] is as shown below:



10.1. Realtime Logs

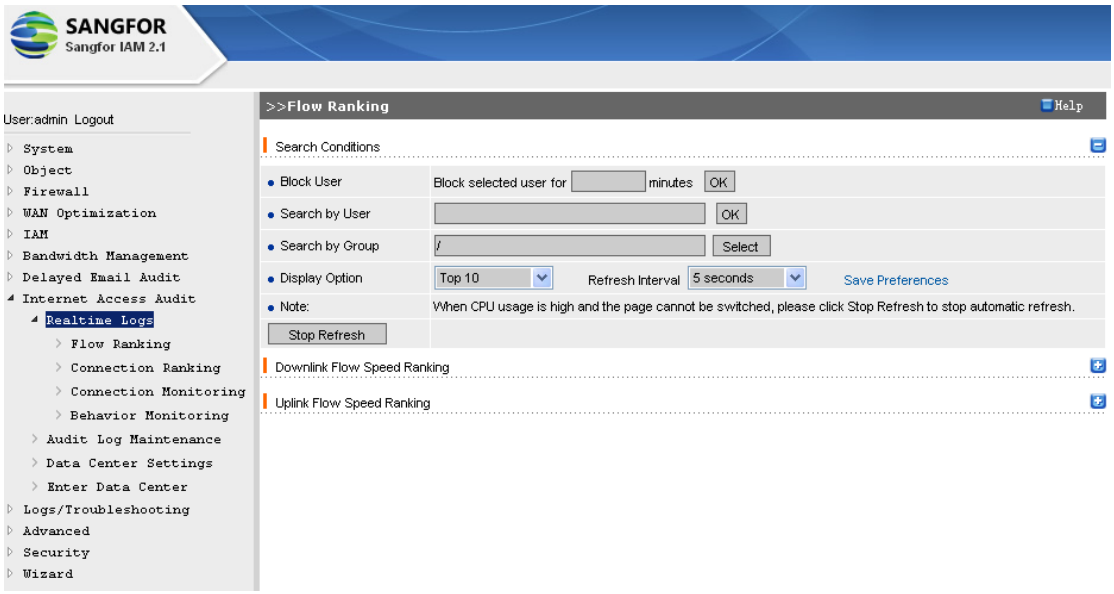
[Realtime Logs] includes the information of [Flow Ranking], [Connection Ranking], [Connection Monitoring] and [Behavior Monitoring].

[Flow Ranking]: Displays the real-time flow information caused by the LAN users getting access to the Internet.

[Connection Ranking]: Displays the number of active connections caused by the LAN users.

[Connection Monitoring]: Displays all the connections that a LAN IP address has established with the external networks.

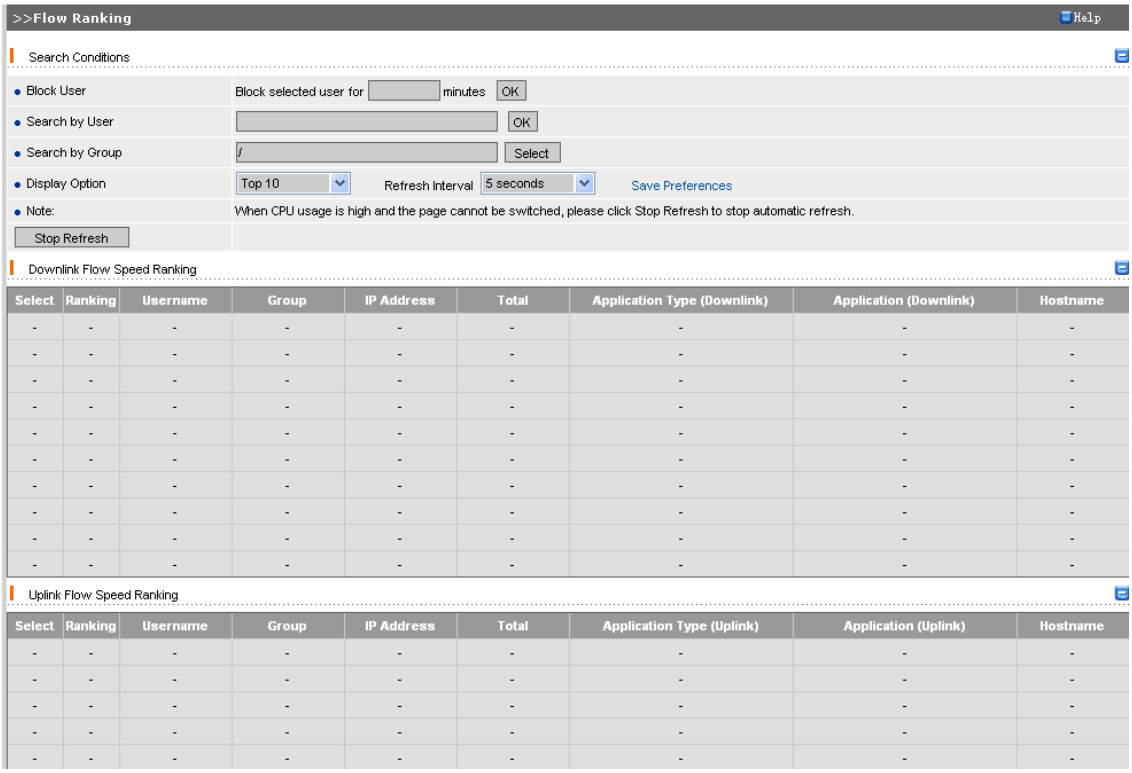
[Behavior Monitoring]: Displays the Internet behavior of a certain LAN IP address, including the information of application type, application, and detailed information.



10.1.1. Flow Ranking

[Flow Ranking] displays the real-time flow information caused by the LAN users getting access to the Internet. You can obtain the host name of an IP address, and block the selected user(s) to get access to the Internet.

The page is as shown below:



[Search by User]: Specifies a user to view its/their flow ranking information.

[Search by Group]: Specifies a group to view the flow ranking information. Click the <Select> button and select a user group, and then click <OK>.

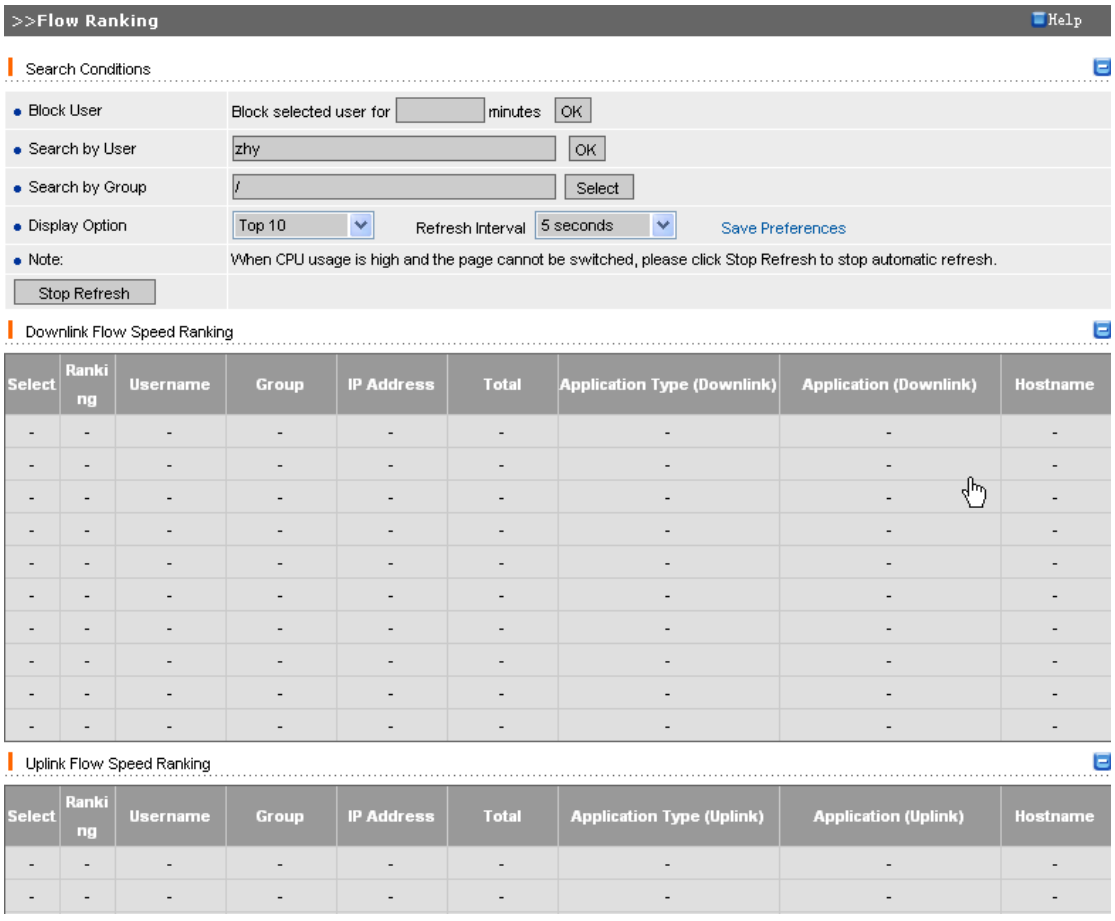
[Display Option]: Specifies the number of items to be displayed (the top flow rankings), and the time interval to automatically refresh the data. You can click <Save Preference> to save the settings and facilitate you to view your preferred statistics (displayed by default) next time.

<Stop Refresh>: Click this button to have the auto refresh function stop.

<Obtain>: Click this button to obtain the host name of the corresponding device (IP address), as shown below:

If you want to block a user, select the user and then configure the time duration which the selected user(s) is blocked for.

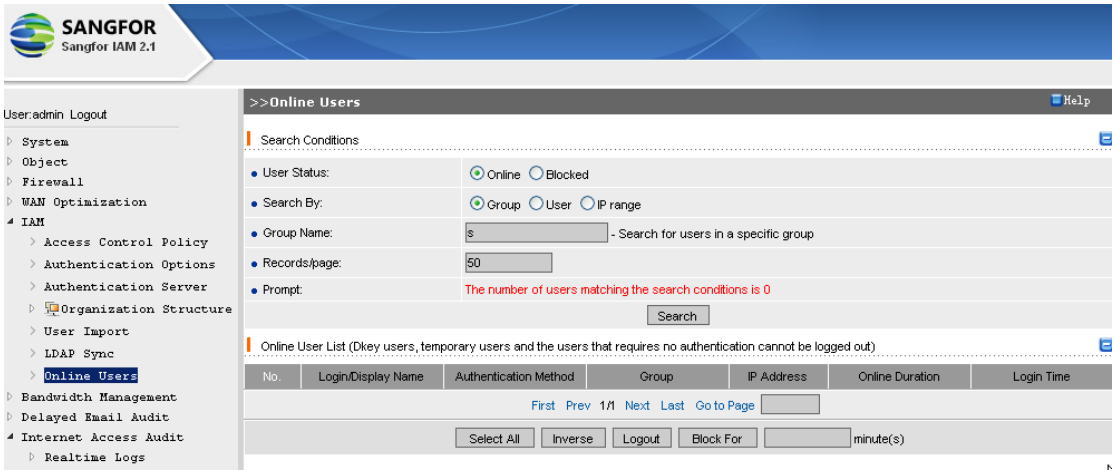
Click the <OK> button, as shown below:



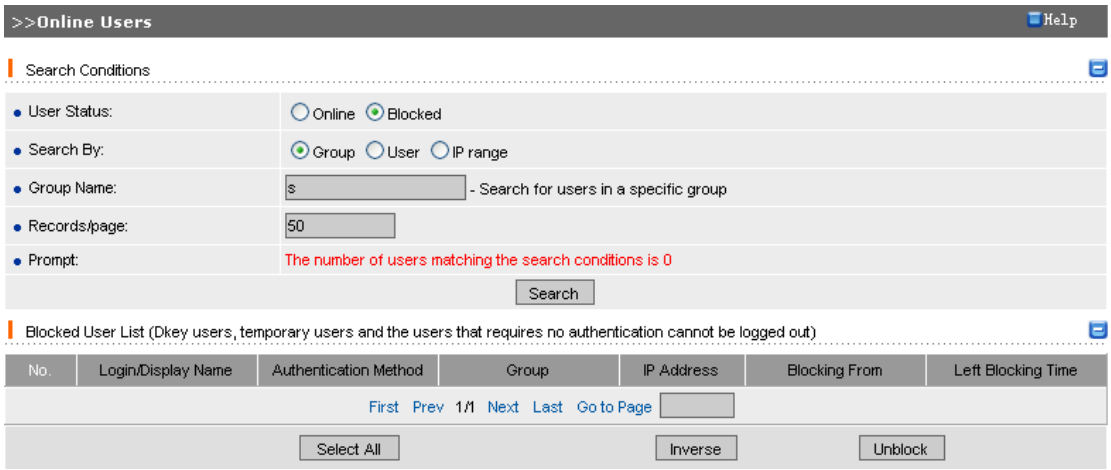
System will prompt that the command for blocking the user is sent successfully.

Click the <Auto Update> button and you will see there is no flow caused by the blocked user (for the user/IP address is blocked from accessing to the Internet).

You search the blocked user(s) in [IAM] > [Online User]; just select [Blocked] and then click the <Search> button.



To unblock a user, just select the user and then click the <Unblock> button.


>>Online Users
Help
Search Conditions
User Status: Online Blocked
Search By: Group User IP range
Group Name: s - Search for users in a specific group
Records/page: 50
Prompt: The number of users matching the search conditions is 0
Search
Blocked User List (Dkey users, temporary users and the users that requires no authentication cannot be logged out)
No. Login/Display Name Authentication Method Group IP Address Blocking From Left Blocking Time
First Prev 1/1 Next Last Go to Page
Select All Inverse Unblock

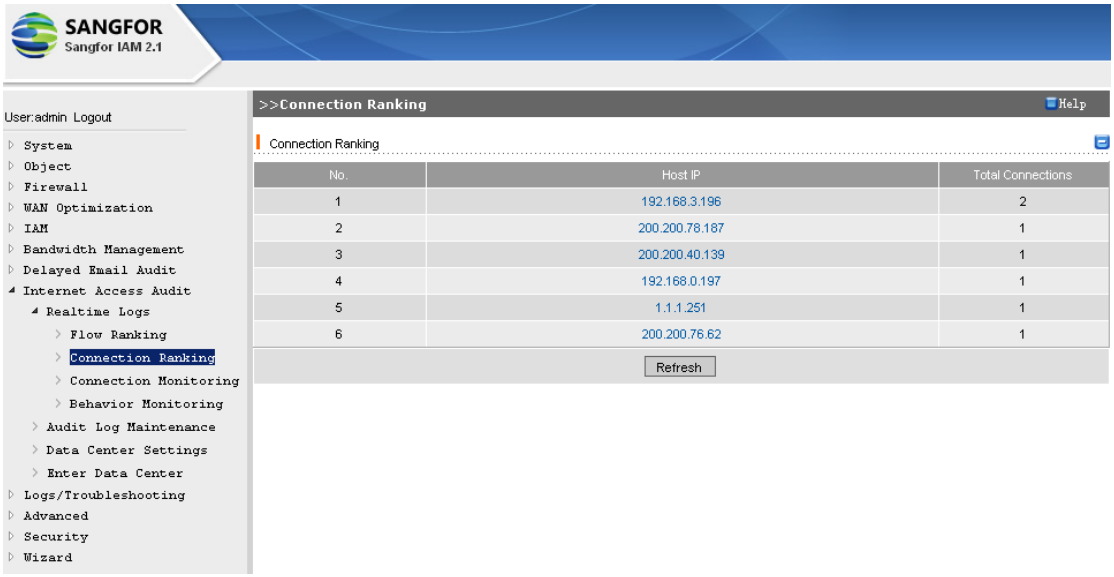
Click the <Auto Update> button and you will see that there is flow caused by the unblocked user (for the user/IP address can access the Internet again).

10.1.2. Connection Ranking

[Connection Ranking] displays the number of active connections caused by the LAN users. It only displays the top 20 connection rankings (IP addresses).

Click the <Refresh> button to view the latest refreshed data of active connections caused by the

LAN users, as shown below:

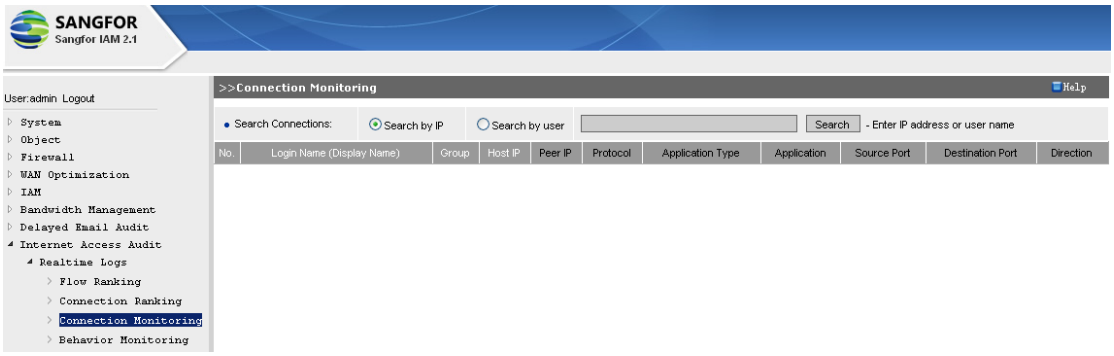


Maximum top 20 connection rankings are displayed.

10.1.3. Connection Monitoring

[Connection Monitoring] displays all the connections that a LAN IP address has established with the external networks. It only displays the top 200 connection rankings (IP addresses).

Under the [Connection Monitoring] page, enter an IP address and click the <Search> button to refresh the displayed connections of this IP address. The page is as shown below:

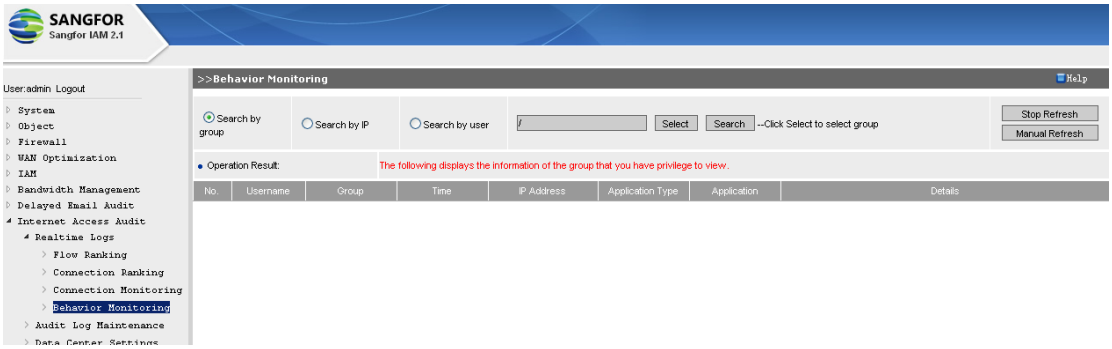


10.1.4. Behavior Monitoring

[Behavior Monitoring] displays the Internet behavior of certain LAN IP address, including the

information of application type, application, and detailed information.

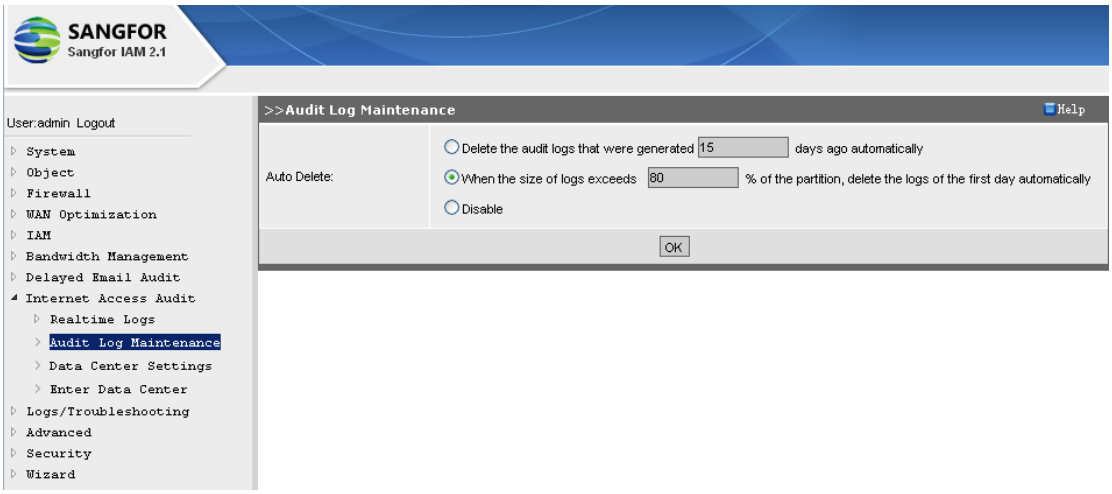
Specify the search condition and click the <Search> button to view the latest Internet behavior of this user (IP address). The page is as shown below:



10.2. Audit Log Maintenance

[Audit Log Maintenance] configures whether to have the system automatically delete the audit logs. Options are [Delete the audit logs that were generated _ days ago automatically], [When the size of logs exceeds _ % of the partition, delete the logs of the first day automatically], and [Disable].

The page is as shown below:

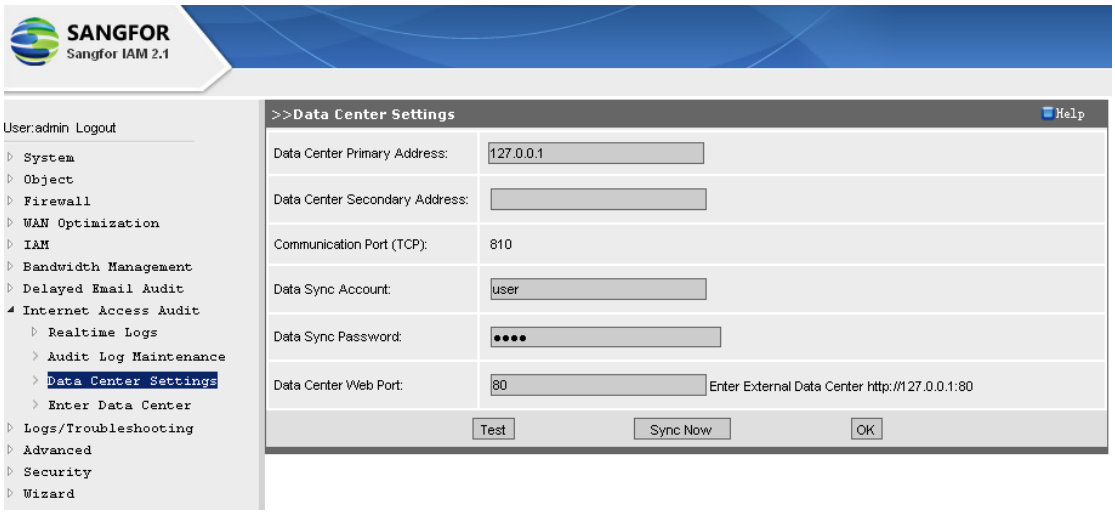


Having completed configuring this page, you have to click the <OK> button to save the settings.

10.3. Data Center Settings

[Data Center Settings] configures the server that synchronizes the logs, including the IP address, account/password, and WEB port of the external Data Center.

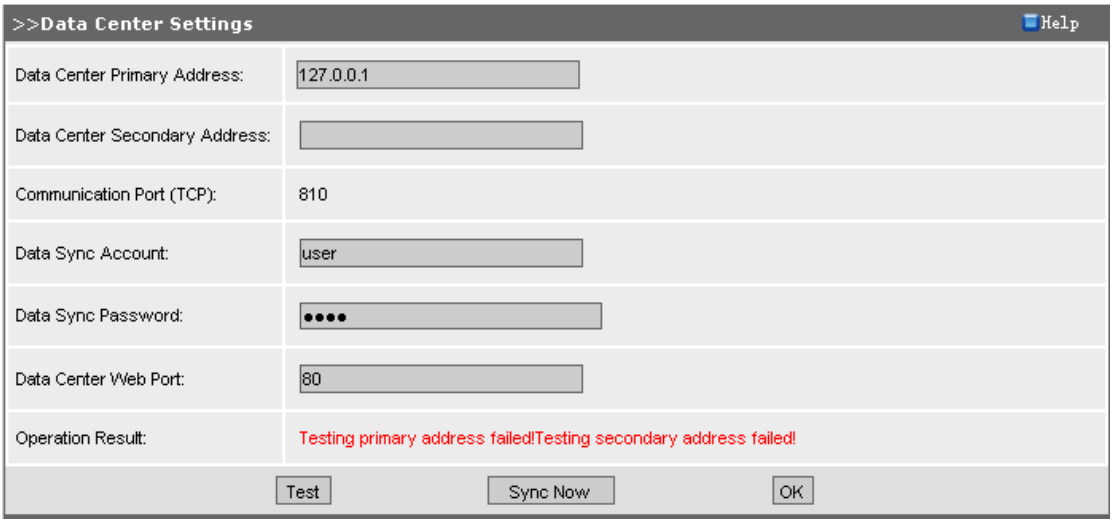
The configuration page is as shown below:



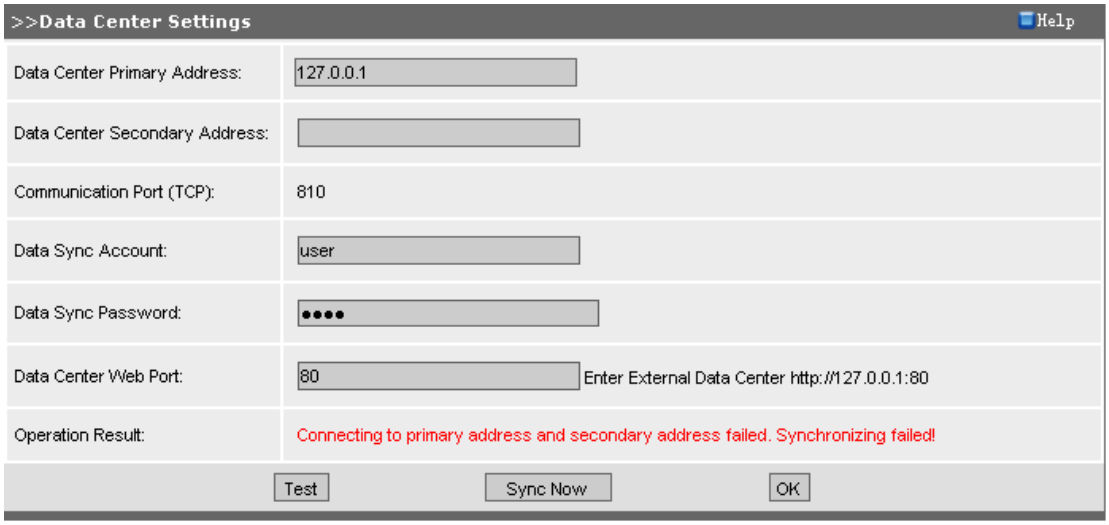
[Data Center Primary Address], [Data Center Secondary Address]: Configures the server IP address of the Data Center of SANGFOR IAM gateway device. The address can be an IP address or the corresponding domain name; ensure that the IAM gateway device can parse the domain name (the IAM gateway should be able to access the Internet).

[Data Sync Account], [Data Sync Password]: Enter the account name and password respectively.

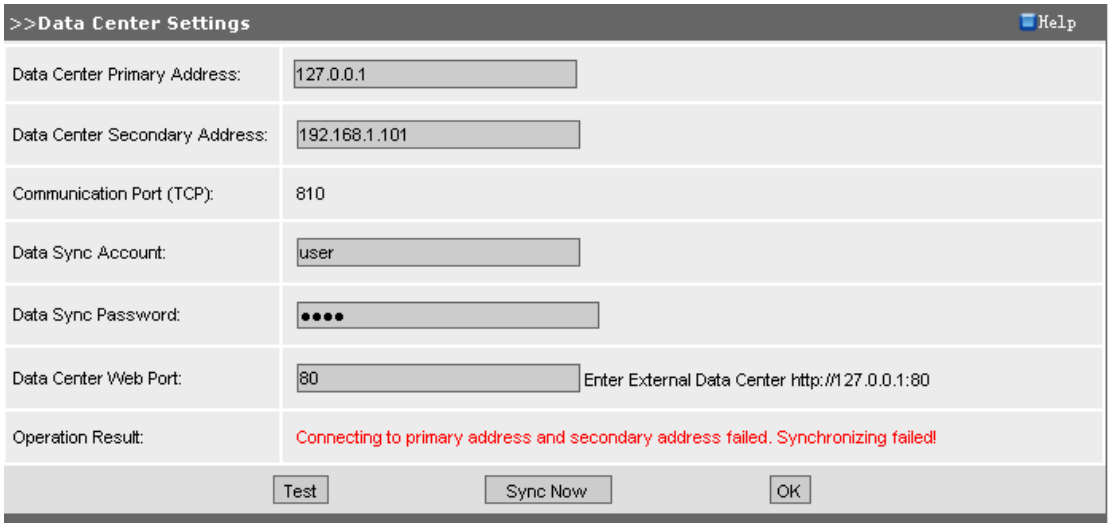
Click the <Test> button to check the connectivity with the server of SANGFOR IAM gateway Data Center.



Click the <Sync Now> button and the IAM gateway will send the synchronization command to the server of the Data Center to synchronize the system logs.



[Data Center Web Port]: Configures the port through which the external Data Center provides WEB services.

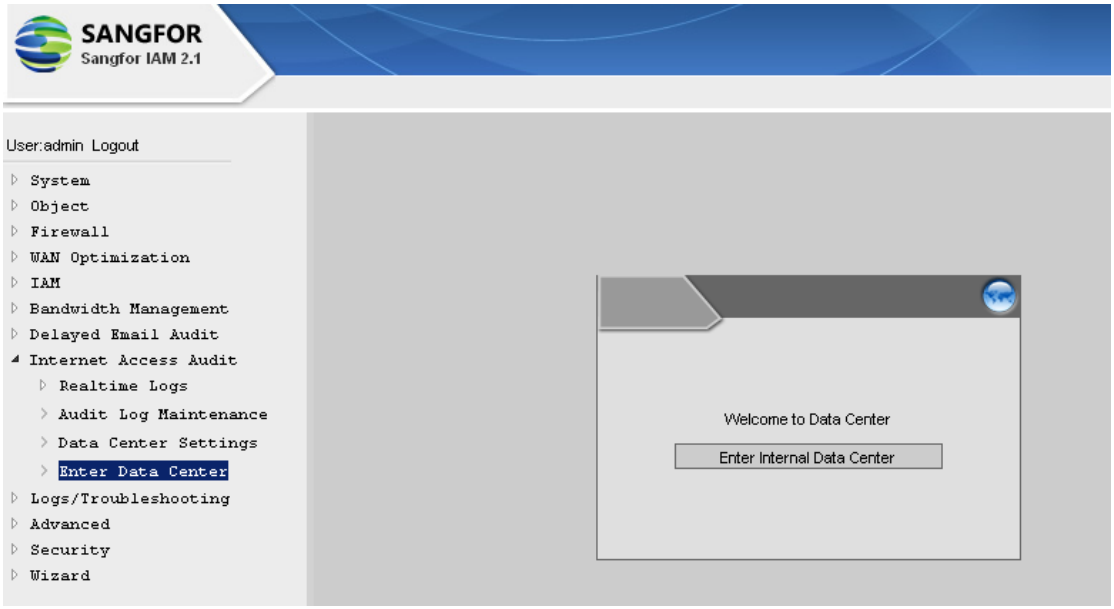


Click the [Enter External Data Center http://IP:PORT] (varies with IP address and port) to enter the login interface of the internal Data Center, as shown below:

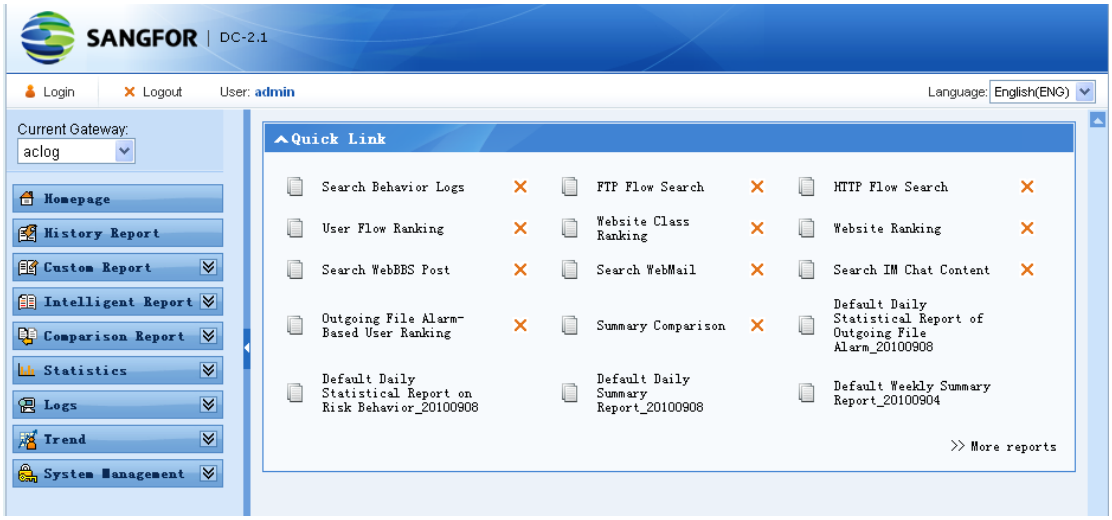
Having completed configuring the page, you have to click the <OK> button to save all the settings.

10.4. Enter Data Center

[Enter Data Center] enables you to log in to the internal Data Center of the IAM gateway device as the present user, to search for the logs and make statistics in real time.



Click the <Internal Data Center> button to log in to the Data Center, as shown below:



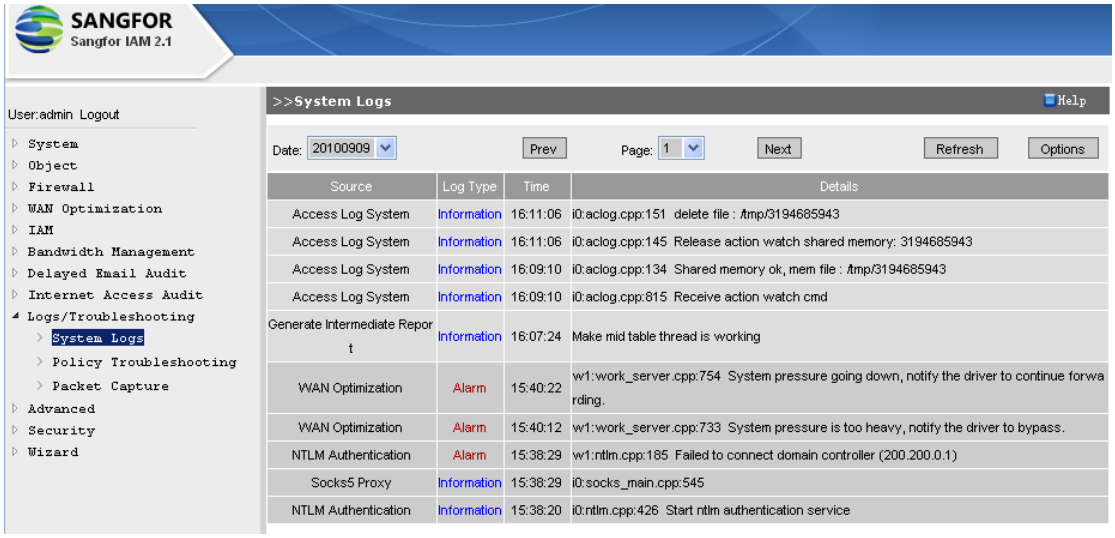
Under the above page, you can make statistics and search for the behavior records of the LAN user, or generate PDF format report according to your needs.

As the storage capacity of the IAM gateway device is limited, and data retrieval and search among massive data records in the Data Center will consume large resources, it is recommended NOT to have the internal Data Center store large amount of data. If your networking produces massive logs, you can install an independent (external) Data Center server to store logs and search for specific data.

Chapter 11 Logs/Troubleshooting

[Logs/Troubleshooting] covers [System Logs], [Policy Troubleshooting] and [Packet Capture].

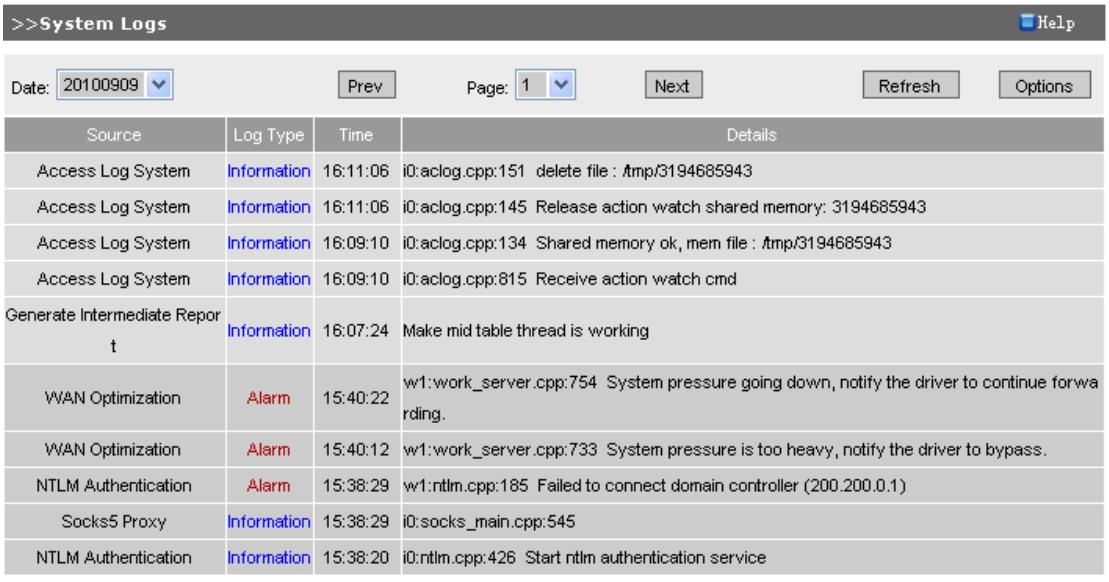
The configuration page is as shown below:



11.1. System Logs

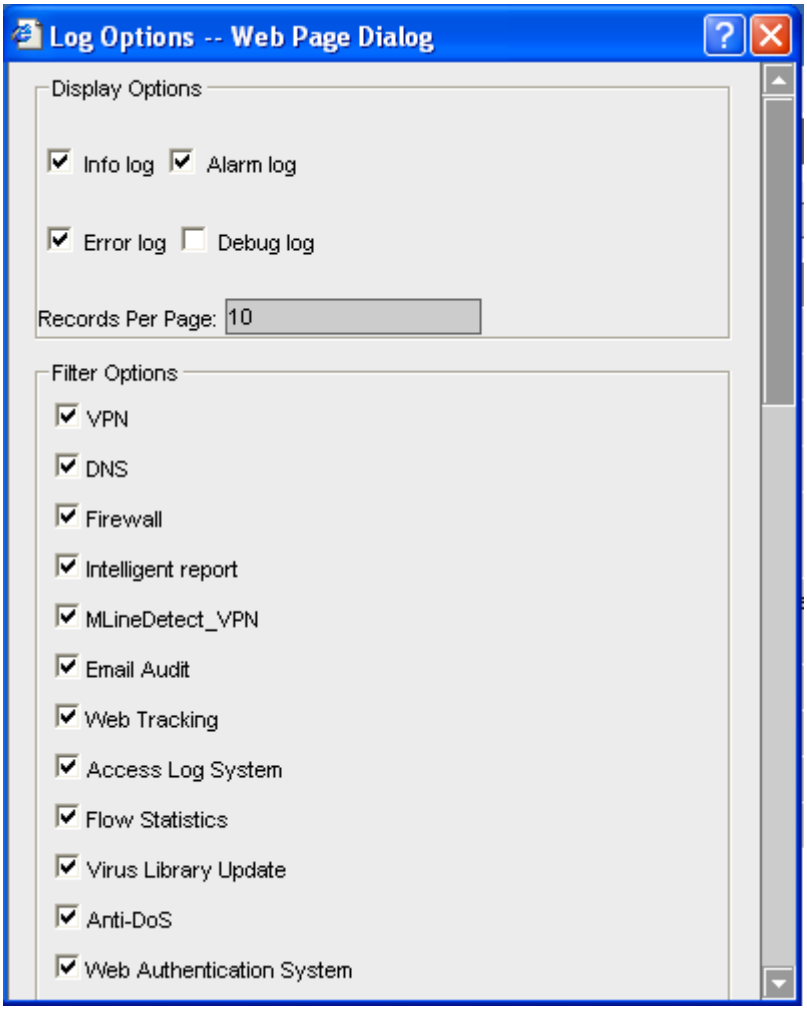
[System Logs] displays the running information of each function module of the IAM gateway device. With the help of these logs, you can tell whether each module is working normally.

The page is as shown below:



Click the <Options> button (at the right top of the interface) to enter the [Log Options] dialog to

define the display of the system logs, as shown below:



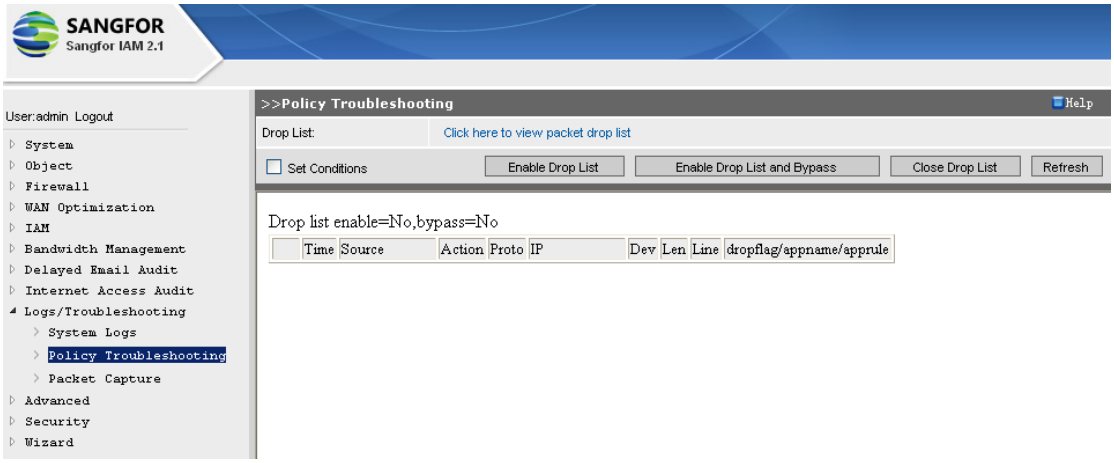
Having completed defining the [Display Options] and [Filter Options], you have to click the <OK> button and then click the <Refresh> button to apply the new configuration, as shown below:

Source	Log Type	Time	Details
WAN Optimization	Alarm	15:40:22	w1:work_server.cpp:754 System pressure going down, notify the driver to continue forwarding.
WAN Optimization	Alarm	15:40:12	w1:work_server.cpp:733 System pressure is too heavy, notify the driver to bypass.
NTLM Authentication	Alarm	15:38:29	w1:ntlm.cpp:185 Failed to connect domain controller (200.200.0.1)
Web Authentication System	Alarm	15:34:06	w1:libcheckcpu.cpp:40 open /proc/18496/cpu failed
HA	Alarm	15:07:53	[cluster]Local device is primary device. Failed to detect secondary device!
HA	Alarm	14:07:53	[cluster]Local device is primary device. Failed to detect secondary device!
HA	Alarm	13:07:53	[cluster]Local device is primary device. Failed to detect secondary device!
NTLM Authentication	Alarm	12:28:33	w1:ntlm.cpp:185 Failed to connect domain controller (200.200.0.1)
NTLM Authentication	Alarm	12:27:32	w1:ntlm.cpp:185 Failed to connect domain controller (200.200.0.1)
HA	Alarm	12:07:54	[cluster]Local device is primary device. Failed to detect secondary device!

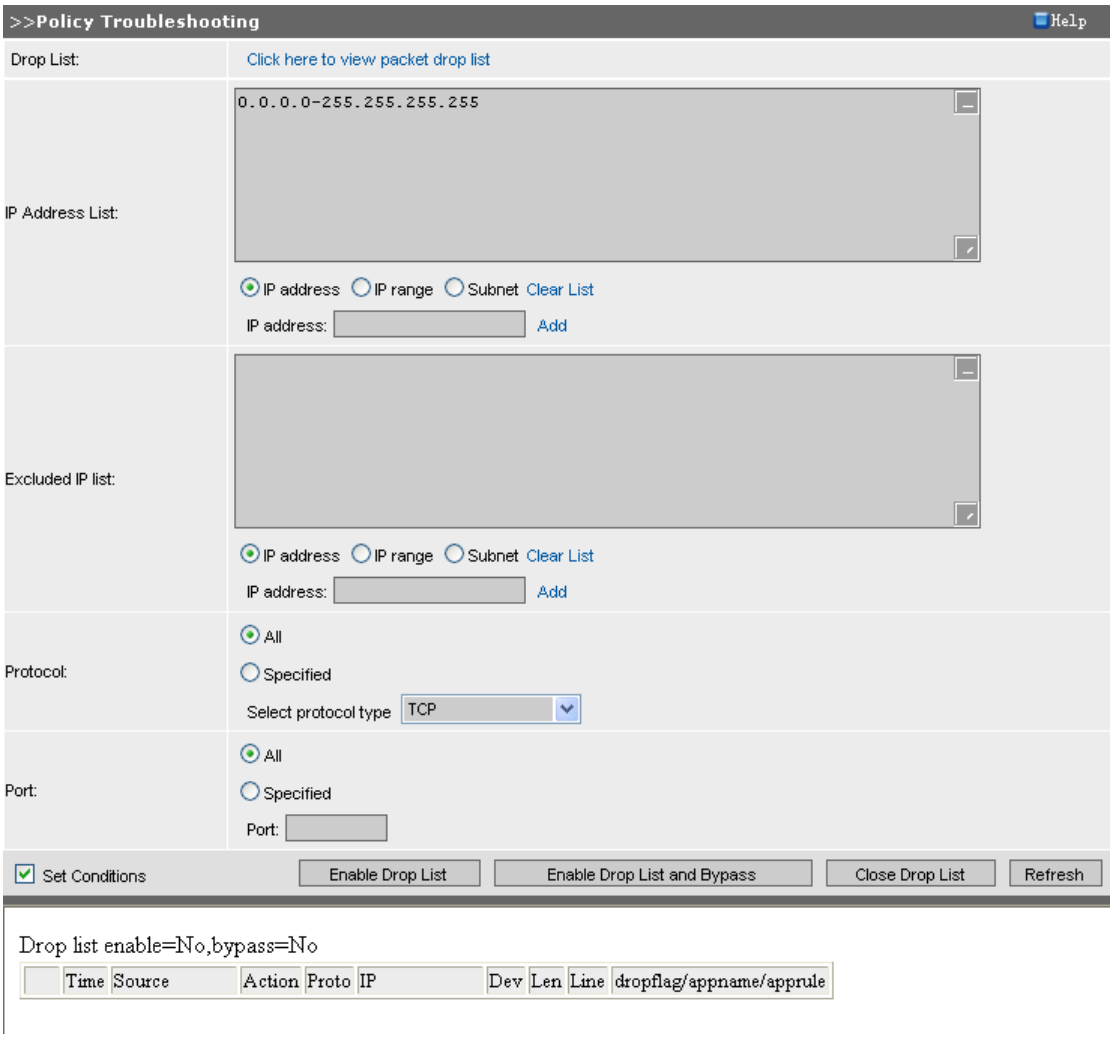
11.2. Policy Troubleshooting

[Policy Troubleshooting] enables you to view which module has denied the data packet, for what reason, so as to locate the configuration mistakes made on certain module or test whether some rules is taking effect or not.

The page is as shown below:



Check the [Set Conditions] to view the conditions items and configure the filtering conditions, such as [IP Address List], [Excluded IP List], [Protocol] and [Port], etc., as shown below:



[IP Address List]: Configures the IP address to which this rule is applied. It defaults to include all the segments.

[Excluded IP List]: Configures the IP address whose data packet will get bypassed but the denied information will be recorded.

[Protocol], [Port]: Configures the protocol condition, that only the protocol and port contained in the transmitted data packet are the configured ones will the denied information be recorded.

Click <Enable Drop List> to enable the Drop list (all the access control policies configured on the IAM gateway device are taking effect), and the packets applicable to the policies (to be denied) will be denied and the related information will be outputted to a WEB page. Click <Click here to view packet drop list> to open the page and view the detailed information of the denied data packets.

Click the <Enable Drop List and Bypass> button to enable the drop list and enable the bypass function (all the access control policies configured on the IAM gateway device will get invalid),

and the data packets applicable to the policy (to be denied) will be let pass and the related information will be outputted to a WEB page. Click the <Click here to view packet drop list> button to open the page and view detailed information of the denied data packets.

This function helps do troubleshooting quickly, locate the configuration mistakes made on certain function module (of the IAM gateway device) which caused faults such as network disconnection, etc., and therefore helps the network administrator to quickly correct the configurations.

<Close Drop List>: Click this button to close the Drop list and disable the bypass function.

The Drop List is as shown below:

Drop list enable=Yes,bypass=Yes

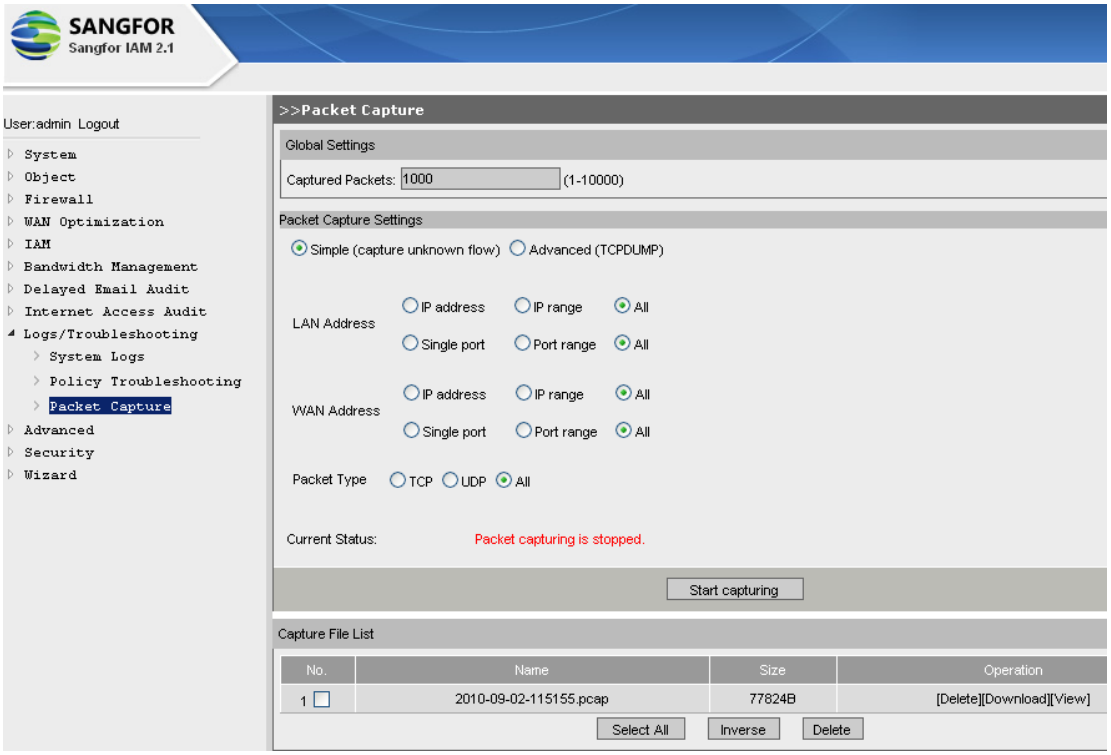
	Time	Source	Action	Proto	IP	Dev	Len	Line	dropflag/ap
061	11:11:19	firewall	(line:2997)this connect has 'been dropped by session flag:20!	tcp	192.168.1.106:2390 -> 124.115.5.231:443	eth0->eth2	40	0	httporssl/Q [S443]
060	11:11:19	firewall	(line:2997)this connect has 'been dropped by session flag:20!	tcp	124.115.5.231:443 -> 192.168.1.106:2390	eth2->eth0	40	0	httporssl/Q [S443]
059	11:11:19	firewall	(line:2997)this connect has 'been dropped by session flag:20!	tcp	124.115.5.231:443 -> 192.168.1.106:2390	eth2->eth0	40	0	httporssl/Q [S443]
058	11:11:19	firewall	(line:2997)this connect has 'been dropped by session flag:20!	tcp	192.168.1.106:2390 -> 124.115.5.231:443	eth0->eth2	40	0	httporssl/Q [S443]
057	11:11:19	firewall	(line:2997)this connect has 'been dropped by session flag:20!	tcp	192.168.1.106:2390 -> 124.115.5.231:443	eth0->eth2	84	0	httporssl/Q [S443]
056	11:11:10	firewall	(line:2997)this connect has 'been dropped by session flag:20!	tcp	192.168.1.106:2390 -> 124.115.5.231:443	eth0->eth2	40	0	httporssl/Q [S443]
055	11:11:10	firewall	(line:2997)this connect has 'been dropped by session flag:20!	tcp	124.115.5.231:443 -> 192.168.1.106:2390	eth2->eth0	90	0	httporssl/Q [S443]

- [Set Conditions] is recommended to be configured. With these conditions, you can filter some irrelevant information and make troubleshooting more accurate and the process simpler.
- After policy troubleshooting, DO remember to close the Drop list, for this function consumes some system resources; what is more, if the bypass function is not disabled, all the policies configured are invalid.

11.3. Packet Capture

[Packet Capture] is used for capturing the data packets that go through the IAM gateway device. This function helps to quick locate configuration mistakes, and is a supplementary troubleshooting tool of policy troubleshooting.

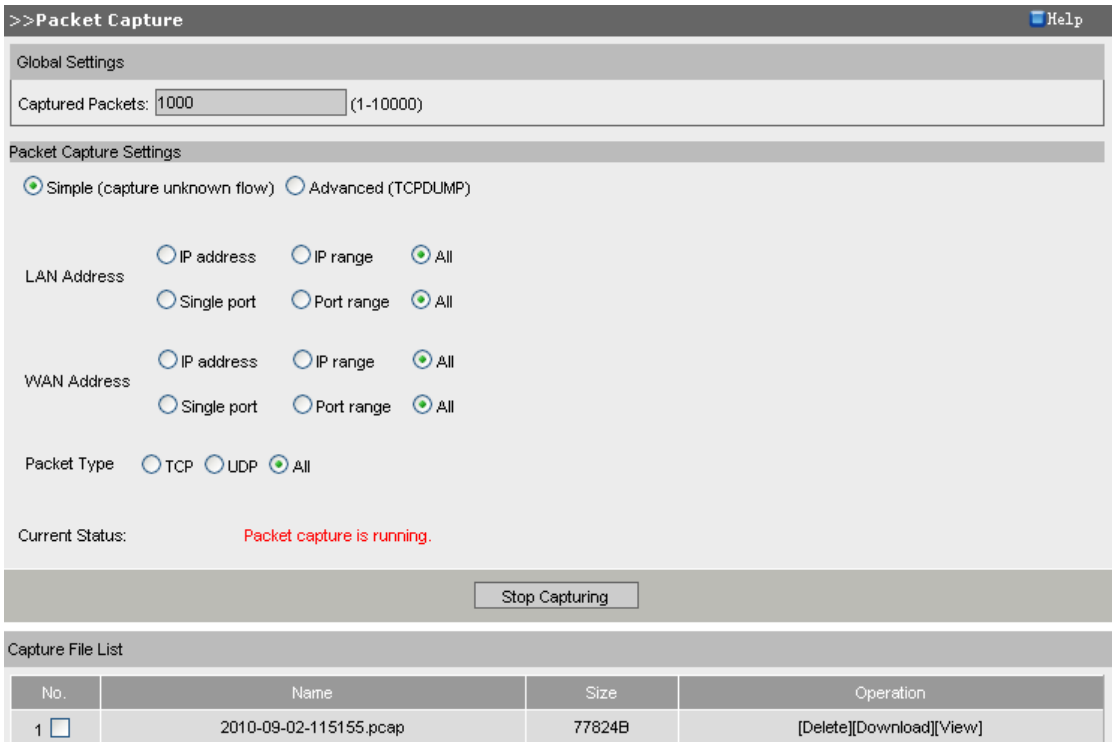
The configuration page is as shown below:



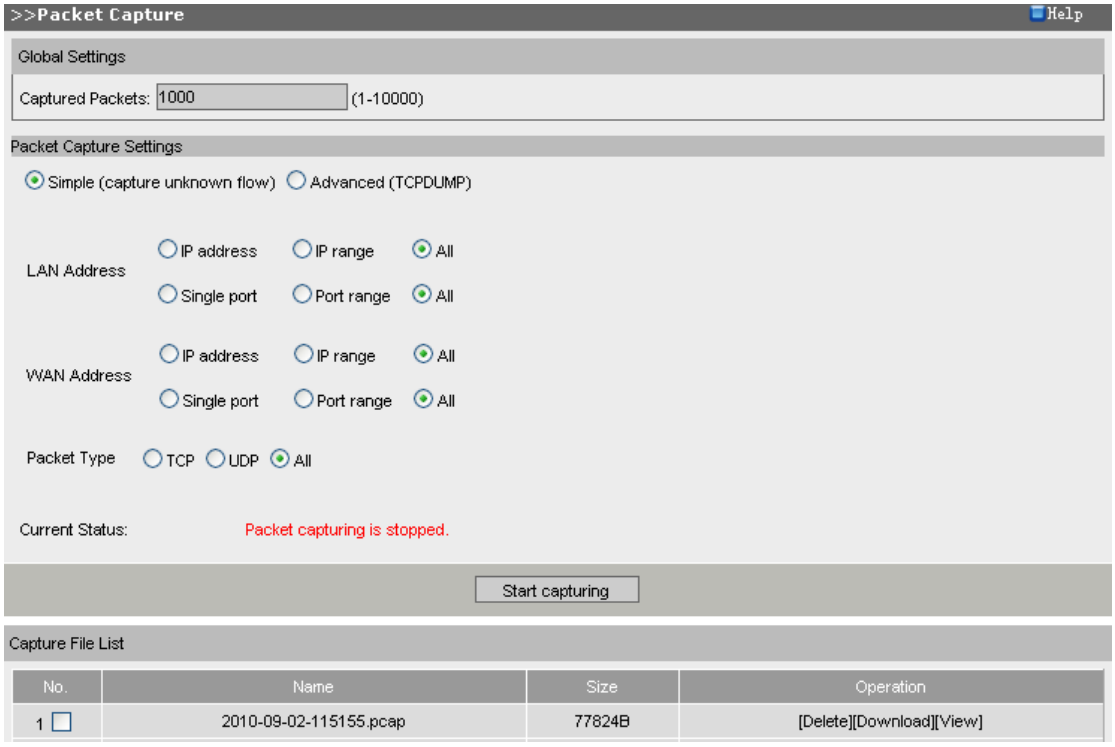
[Capture Packets]: Configures the total number the packets to be captured.

[Simple (capture unknown flow)]: Select this item and configure the conditions such as the source LAN IP address and port, WAN destination IP and port, and packet type. It will capture the matching data packets of the unknown applications.

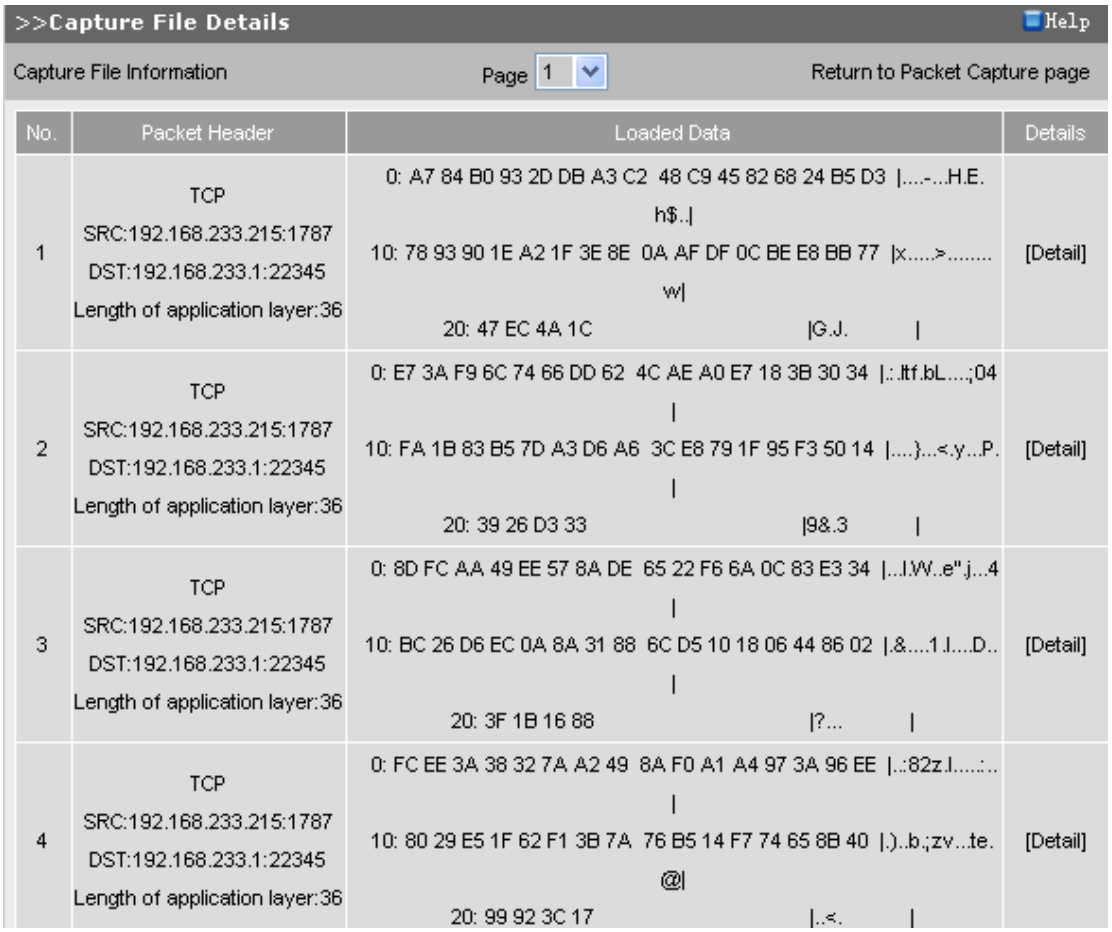
Click the <Start capturing> button to have it start capturing the data packets, as shown below:



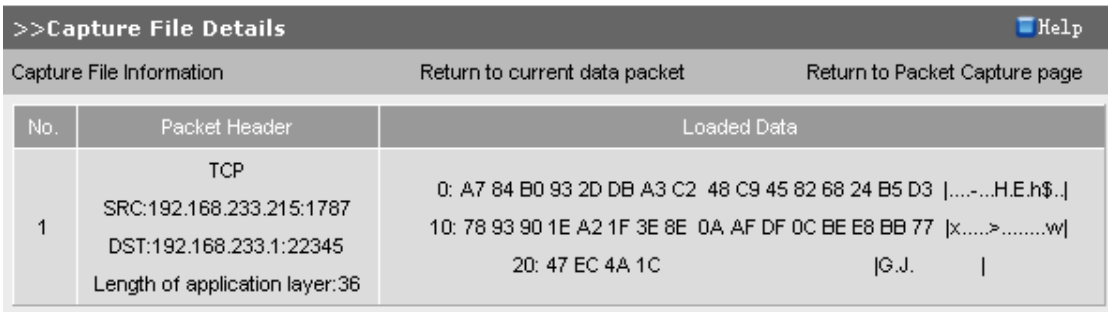
Click the <Stop capturing> button to have it stop capturing the data packets. And then you will see a captured file (with the file extension pcap) in the [Capture File List], as shown below:



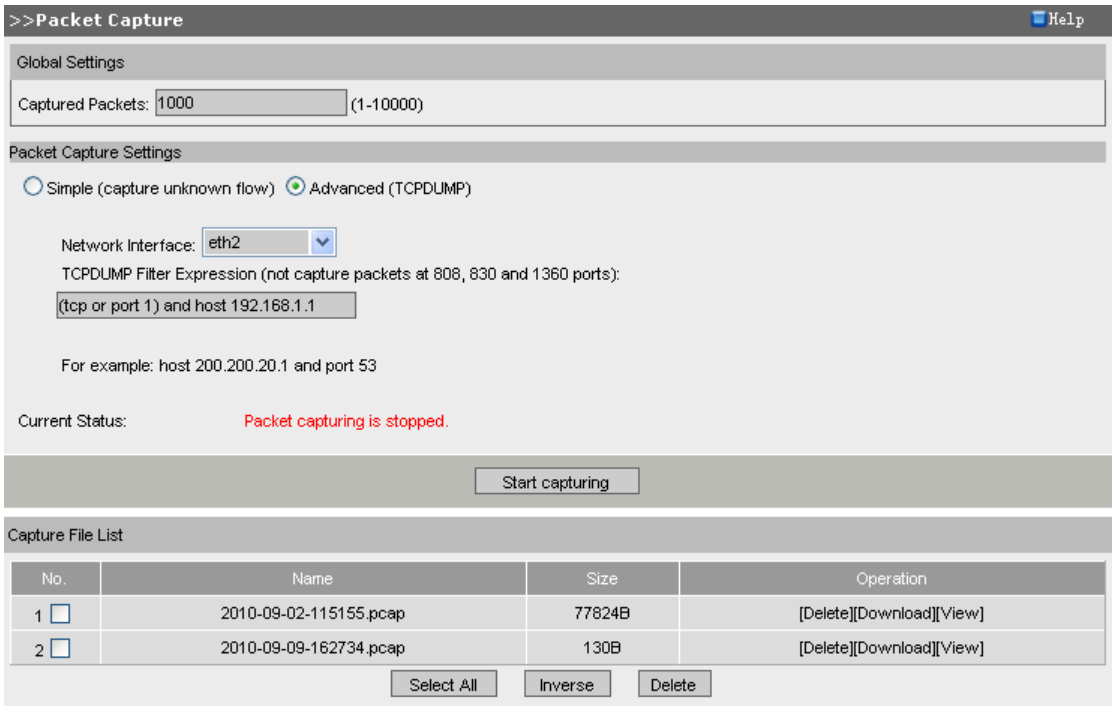
Click <View> to open the [Capture File Details] page, as shown below:


>>Capture File Details
Help
Capture File Information
Page 1
Return to Packet Capture page
No.
Packet Header
Loaded Data
Details
1
TCP
SRC:192.168.233.215:1787
DST:192.168.233.1:22345
Length of application layer:36
0: A7 84 B0 93 2D DB A3 C2 48 C9 45 82 68 24 B5 D3 |....-...H.E.h$..|
10: 78 93 90 1E A2 1F 3E 8E 0A AF DF 0C BE E8 BB 77 |x.....>.....w|
20: 47 EC 4A 1C |G.J. |
[Detail]
2
TCP
SRC:192.168.233.215:1787
DST:192.168.233.1:22345
Length of application layer:36
0: E7 3A F9 6C 74 66 DD 62 4C AE A0 E7 18 3B 30 34 |.:.ltf.bL....;04|
10: FA 1B 83 B5 7D A3 D6 A6 3C E8 79 1F 95 F3 50 14 |....}...<.y...P.|
20: 39 26 D3 33 |9&.3 |
[Detail]
3
TCP
SRC:192.168.233.215:1787
DST:192.168.233.1:22345
Length of application layer:36
0: 8D FC AA 49 EE 57 8A DE 65 22 F6 6A 0C 83 E3 34 |...I.W..e"j...4|
10: BC 26 D6 EC 0A 8A 31 88 6C D5 10 18 06 44 86 02 |.&....1.l....D..|
20: 3F 1B 16 88 |?... |
[Detail]
4
TCP
SRC:192.168.233.215:1787
DST:192.168.233.1:22345
Length of application layer:36
0: FC EE 3A 38 32 7A A2 49 8A F0 A1 A4 97 3A 96 EE |..:82z.I.....:..|
10: 80 29 E5 1F 62 F1 3B 7A 76 B5 14 F7 74 65 8B 40 |.)..b.;zv...te.@|
20: 99 92 3C 17 |..<. |
[Detail]

Click <Details> to view the detailed data loaded by the data packets, as shown below:


>>Capture File Details
Help
Capture File Information
Return to current data packet
Return to Packet Capture page
No.
Packet Header
Loaded Data
1
TCP
SRC:192.168.233.215:1787
DST:192.168.233.1:22345
Length of application layer:36
0: A7 84 B0 93 2D DB A3 C2 48 C9 45 82 68 24 B5 D3 |....-...H.E.h$..|
10: 78 93 90 1E A2 1F 3E 8E 0A AF DF 0C BE E8 BB 77 |x.....>.....w|
20: 47 EC 4A 1C |G.J. |

[Advanced (TCPDUMP)]: Select this item and configure the conditions such as network interface and TCPDUMP filter expression which helps to capture data packets, as shown below:



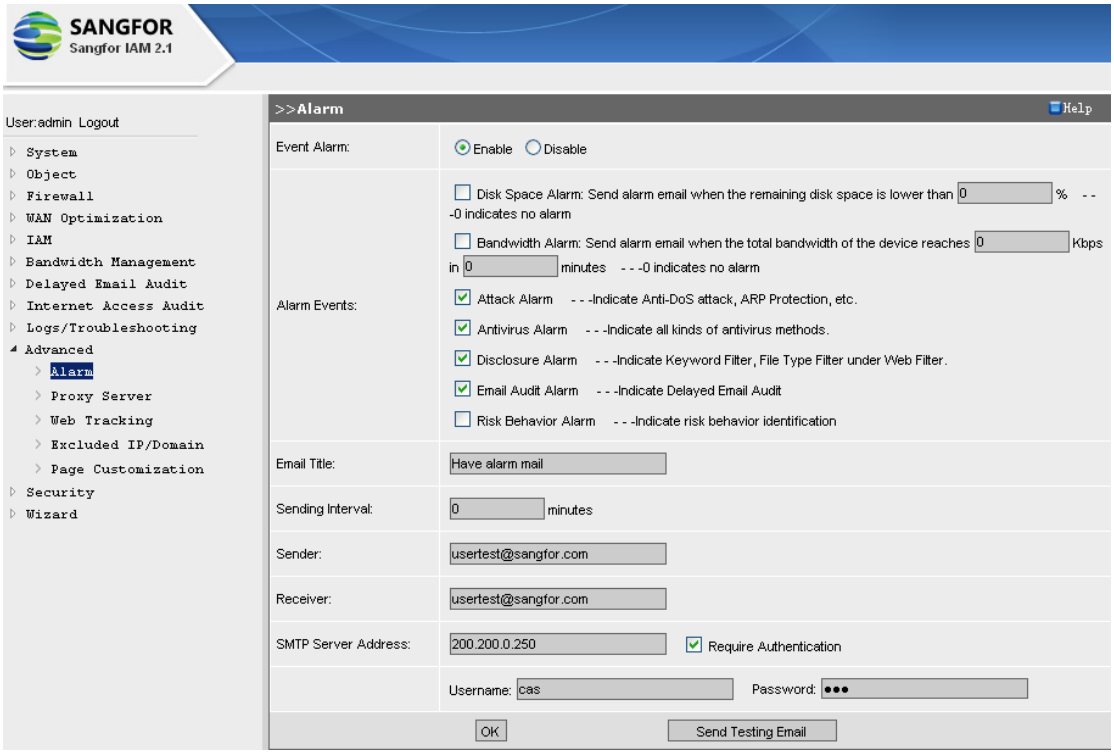
Click the <Delete> button to delete a selected captured file, or click <Download> to save the file into a specified file path of the local computer. This captured file can be opened by the software such as Sniffer, Ethereal, etc.

Chapter 12 Advanced

[Advanced] covers the configurations of [Alarm], [Proxy Server], [Web Tracking], [Excluded IP/Domain] and [Page Customization].

12.1. Alarm

[Alarm] is used for sending alarm emails to the administrator if the IAM gateway device detects attack, virus, and file disclosure, to-be-audited email and risky behavior.



[Event Alarm]: Select [Enable] to enable the event alarm function. This is an overall switch for the alarm function only with which will the email alarm function take effect.

[Alarm Events]: Includes [Disk Space Alarm], [Bandwidth Alarm], [Attack Alarm], [Antivirus Alarm], [Disclosure Alarm], [Email Audit Alarm] and [Risk Behavior Alarm]. You can check one or more options according to your needs.

[Email Title]: Defines the title of the alarm emails(s).

[Sender]: Configures the email address of the sender that is to send alarm emails.

[Receiver]: Configures the email address of the receiver that is to receive the information of the alarm events and the to-be-audited emails.

[SMTP Server Address]: Configures the IP address or domain name of the SMTP server used for delivering alarm emails.

[Username], [Password]: Type the username and password if the SMTP server requires authentication.

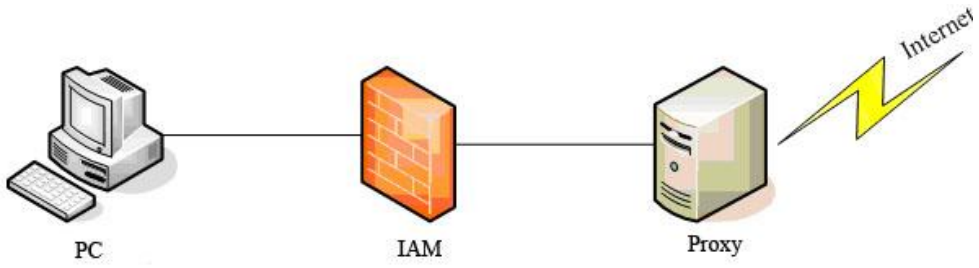
Having completed configuring this page, you can click the <Send Testing Email> button to check whether the email can be delivered successfully.

12.2. Proxy Server

In some cases, the users of the IAM gateway get access to the Internet through proxy. These users are escaping the rules configured on the firewall module, as the firewall module decides whether to allow or deny the data packet only according to the destination address and port.

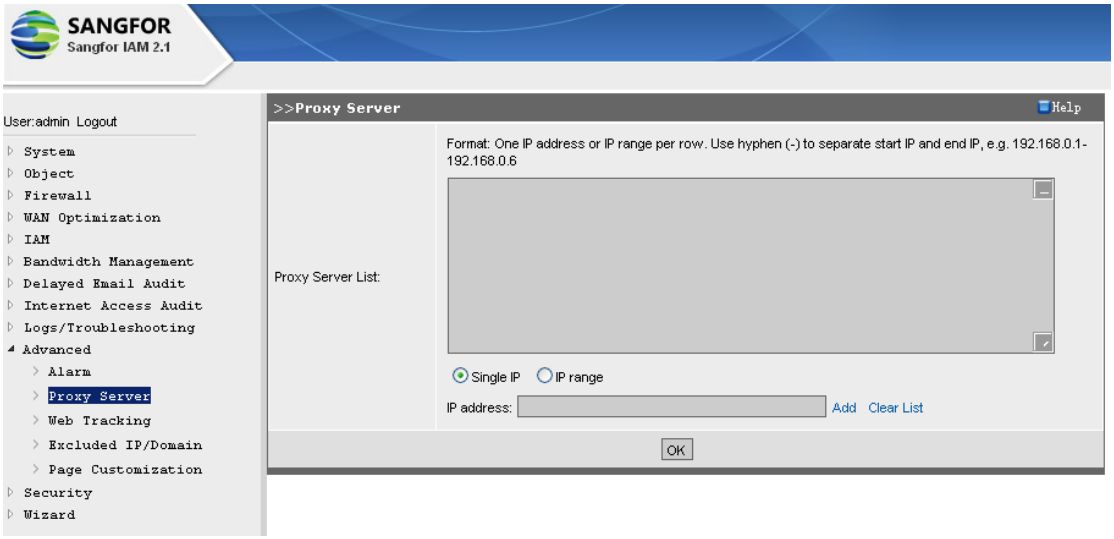
To have the firewall module function, we first need to have the IAM gateway device to analyze the real IP address and port through which the data packets are forwarded by the proxy, and then enable the firewall to get the information.

The networking should be designed as that in the following figure:



The data packet must be ensured to go through the IAM gateway device before being forwarded to the proxy, that is to say, the proxy should be at the WAN interface end of the IAM gateway device.

The configuration page is as shown below:

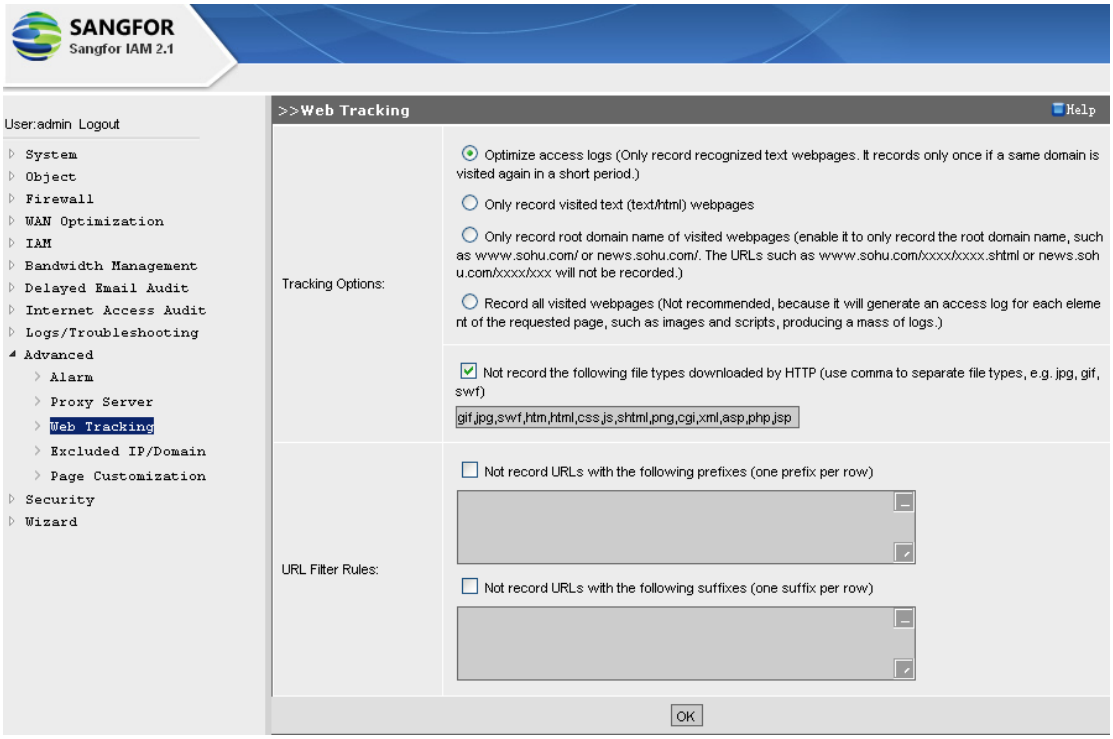


[Proxy Server List]: Enter the IP address or IP ranges of the proxy in this text box. That means the data forwarded to these proxies (IP addresses) will be detected, and thus the administrator can control the Internet access of the LAN users. If the list is blank, all the data forwarded to any proxy will be detected; however, that will surely slower down the processing speed of the IAM gateway device. It is recommended to fill in the IP addresses of some relevant proxies.

- To ensure the data go through the IAM gateway device first and then through the proxy is to ensure that the Proxy is located at the WAN interface end of the IAM gateway device.
- This function does not support the Proxies that require password authentication.

12.3. Web Tracking

[Web Tracking] options define how detailed the logs are audited by the IAM gateway device.


SANGFOR
Sangfor IAM 2.1
User:admin Logout
System
Object
Firewall
WAN Optimization
IAM
Bandwidth Management
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Alarm
Proxy Server
Web Tracking
Excluded IP/Domain
Page Customization
Security
Wizard
>>Web Tracking
Help
Tracking Options:
Optimize access logs (Only record recognized text webpages. It records only once if a same domain is visited again in a short period.)
Only record visited text (text/html) webpages
Only record root domain name of visited webpages (enable it to only record the root domain name, such as www.sohu.com/ or news.sohu.com/. The URLs such as www.sohu.com/xxxx/xxxx.shtml or news.sohu.com/xxxx/xxx will not be recorded.)
Record all visited webpages (Not recommended, because it will generate an access log for each element of the requested page, such as images and scripts, producing a mass of logs.)
Not record the following file types downloaded by HTTP (use comma to separate file types, e.g. jpg, gif, swf)
gif,jpg,swf,htm,html,css,js,shtml,png,cgi,xml,asp,php,jsp
URL Filter Rules:
Not record URLs with the following prefixes (one prefix per row)
Not record URLs with the following suffixes (one suffix per row)
OK

You can define whether to record the URL in detail, or record only the visits to text webpages, or record the download of all HTTP file types, or record the URLs that contain certain prefix or suffix.

[Optimize access logs]: Select this option and it only records the text webpage (only once if a same domain is visited again in a short period).

[Only record visited text (text/html) webpages]: Select this option and it only records the access to text Webpage; otherwise, it records the accesses to all the types of webpages.

[Only record root domain name of visited webpages]: Select this option and it will not record URL in detail, but only the root of the URL. If you want to have it record the full URL, DO NOT select this option.

[Record all visited webpages]: Select this option and it will record every request, and thus produce large number of logs. This option is not recommended.

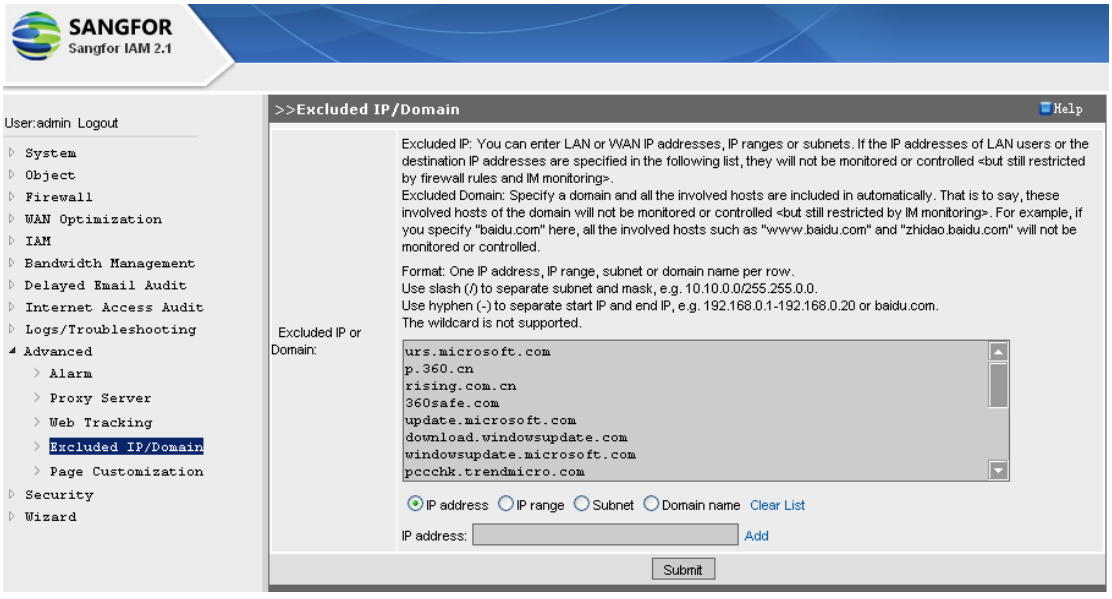
[Not record the following file types downloaded by HTTP]: Check this option and type the file types in the text box. It will record the download of all the filled-in HTTP file types. Different file types are separated from each other by a comma.

[Not record URLs with the following prefixes (one prefix per row)]: Check this option and it will not record the URLs that contain any of the following prefixes configured. The prefix may be matched incompletely. Wildcard are not supported.

[Not record URLs with the following suffixes (one suffix per row)]: Check this option and it will not record the URLs what contain any of the following suffixes configured. The suffix may be matched incompletely. Wildcard are not supported.

- If both the [Not record URLs with the following prefixes (one prefix per row)] and the [Not record URLs with the following suffixes (one suffix per row)] options are checked, these two URL filter rules are of "OR" relationship. That is to say, if either of them is satisfied, the URL will not be audited (recorded).
- A prefix matches a URL from the first character; it may be incompletely matched, and does not support wildcard. For instance, if one of the prefixes configured is "www.s", the URLs such as www.sina.com.cn, www.sohu.com, will not be audited (recorded).
- A suffix matches a URL from the end of it. It may be incompletely matched, and do not support wildcard.

12.4. Excluded IP/Domain


SANGFOR
Sangfor IAM 2.1
User:admin Logout
System
Object
Firewall
WAN Optimization
IAM
Bandwidth Management
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Alarm
Proxy Server
Web Tracking
Excluded IP/Domain
Page Customization
Security
Wizard
>>Excluded IP/Domain
Help
Excluded IP: You can enter LAN or WAN IP addresses, IP ranges or subnets. If the IP addresses of LAN users or the destination IP addresses are specified in the following list, they will not be monitored or controlled <but still restricted by firewall rules and IM monitoring>.
Excluded Domain: Specify a domain and all the involved hosts are included in automatically. That is to say, these involved hosts of the domain will not be monitored or controlled <but still restricted by IM monitoring>. For example, if you specify "baidu.com" here, all the involved hosts such as "www.baidu.com" and "zhidao.baidu.com" will not be monitored or controlled.
Format: One IP address, IP range, subnet or domain name per row.
Use slash (/) to separate subnet and mask, e.g. 10.10.0.0/255.255.0.0.
Use hyphen (-) to separate start IP and end IP, e.g. 192.168.0.1-192.168.0.20 or baidu.com.
The wildcard is not supported.
Excluded IP or Domain:
urs.microsoft.com
p.360.cn
rising.com.cn
360safe.com
update.microsoft.com
download.windowsupdate.com
windowsupdate.microsoft.com
pccchk.trendmicro.com
IP address
IP range
Subnet
Domain name
Clear List
IP address:
Add
Submit

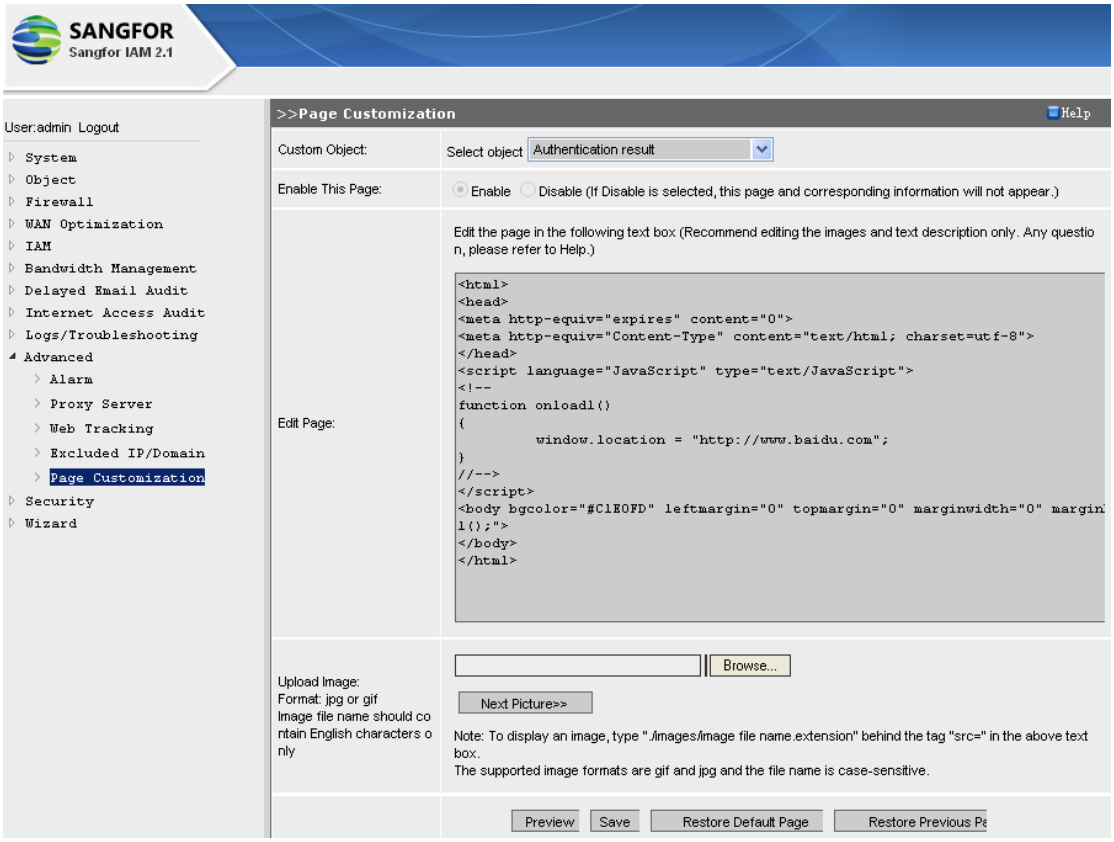
[Excluded IP/Domain]: If the IP address/domain name of a LAN user or the destination IP address

(of a server) is any of the IP addresses/domain names configured here, the Internet access of the LAN user or the visits to the destination server will not be monitored. The data packets will get passed directly.

- If the firewall has configured a rule on any of the IP addresses that are involved in the exclusion rule, the firewall rule has higher priority.
- As the IP address of IM (instant message) server may vary from time to time, it is impossible to absolutely free the IM from monitoring with the exclusion policy configured here.

12.5. Page Customization

[Page Customization] enables you to design some pages to output prompt such as authentication results, access denied, virus detected, Internet access timeout, network ingress client, modify user password, bulletin file, etc.



[Custom Object]: Select a needed object (page). Options are [Authentication Results], [Access Denied], [Virus Detected], [Internet Access Timeout], [Network Ingress Client], [Modify User Password], [Bulletin File], [Web Authentication], [Online Duration Reminder], [Internet Flow Reminder], [PC Proxy Prompt] and [Anti-proxy Reminder].

[Enable This Page]: You are recommended to check [Enable]. If [Disable] is checked, the corresponding prompt page will not pop up.

[Edit Page]: There are codes of some pages provided by the IAM gateway device. You can modify the codes to define the prompt page. You are recommended to only modify the words and pictures displayed on the page. Modification on other parts may result in failure of the links.

[Upload Image]: To insert a picture into the page, click the <Browse> button to upload the picture (only jpg and gif formats supported). Picture name consists of only English characters.

Having configured the above, you can <Preview> the page, <Save> the currently defined page, <Restore Previous Page> or <Restore Default Page>.

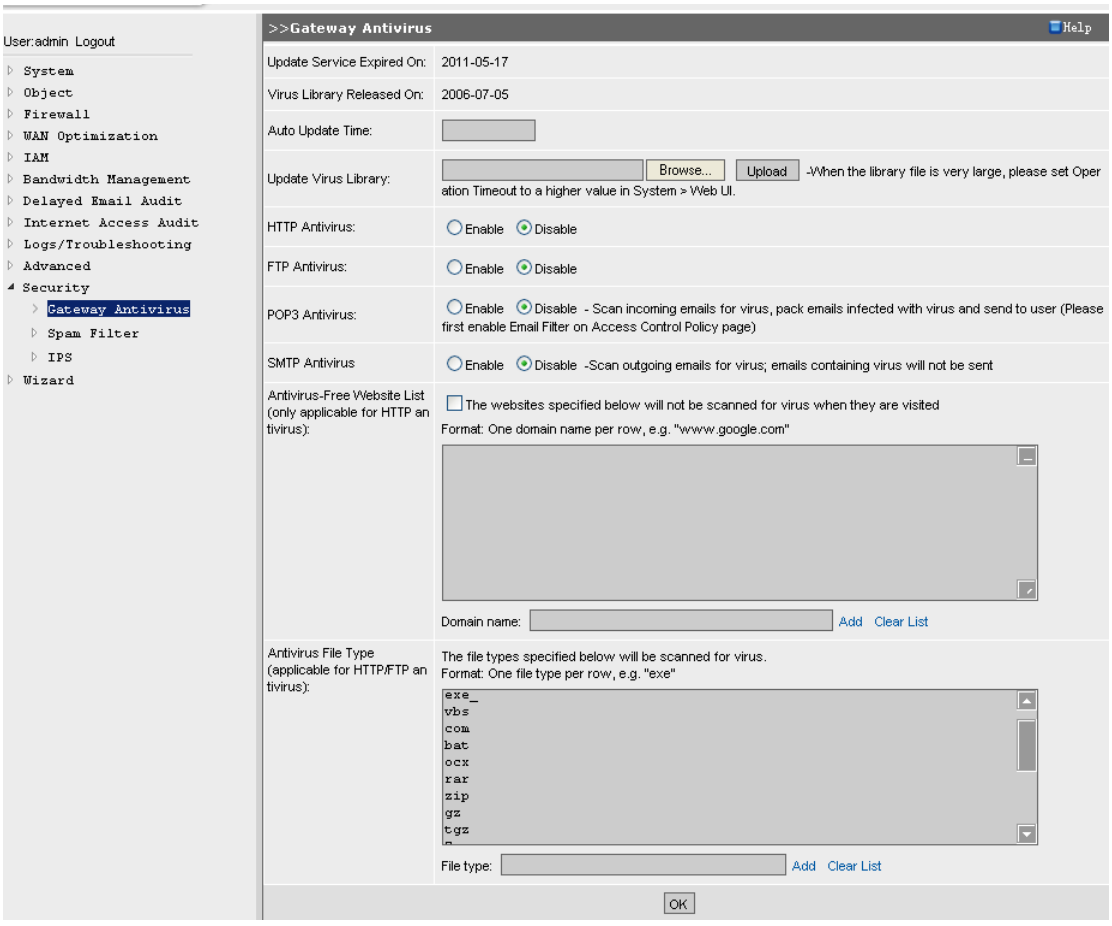
Chapter 13 Security

13.1. Gateway Antivirus

Gateway Antivirus is used for detecting and removing the virus contained in the data packets that are going through the IAM gateway device, and thus to assure the security of the LAN computers. Antivirus system of the IAM gateway is applicable to four common protocols, namely, HTTP, FTP, POP3 and SMTP. The IAM gateway is built in with a well-known antivirus engine by the Iceland provider F-PROT that has high detection rate and effectiveness. The internal virus library of the IAM gateway device updates together with the virus library of F-PROT, generally in 1~2 days.

Under the [Gateway Antivirus] configuration page, you can view the expiry date of the update service, release date of the current version, in addition to configuring the auto update time, importing virus library, enabling antivirus function against the four protocols and configuring the antivirus-free website list and antivirus file type.

The displayed [Virus Library Released On], [Update Service Expired On] and [Auto Update Time] is as shown below:



[Update Service Expired On]: Displays the expiry date of antivirus update service of the IAM gateway device. Within the expiry date, the IAM gateway device will automatically connect the website *http://www.sangfor.com* to update the virus library.

[Virus Library Released On]: Displays the issue date of the current version of virus library.

[Auto Update Time]: Displays the exact time each day when the IAM gateway device shut down for auto-updating the virus library.

[HTTP Antivirus], [FTP Antivirus], [POP3 Antivirus], [SMTP Antivirus]: Select [Enable] to enable the antivirus function against the four protocols respectively.

[Antivirus-Free Website List (only applicable for HTTP antivirus)]: Configures the website(s) that is free from antivirus detecting. Enter the domain name, one entry per row, wildcard not supported.

[Antivirus File Type (applicable for HTTP/FTP antivirus)]: Configures the file extensions of the file(s) that are to be detected by the antivirus software.

- Once the antivirus function gets expired, the virus library can neither be updated automatically nor be updated manually, though the antivirus function still works.
- POP3 antivirus and SMTP antivirus is realized by the proxy function of the IAM gateway device. For this reason, the IAM gateway device must be able to get access to the Internet.
- As to the trusted websites, you can add them to the [Antivirus-Free Website List (only applicable for HTTP antivirus)]. What is more, if a LAN computer need visit the website of the antivirus software provider to update the antivirus software, this antivirus software provider should be added to this list. Because, during the updating process, the downloaded virus library will feature as virus, and the IAM gateway device will mistakenly take the virus library as virus, which disables the LAN computer to update its antivirus software.
- If an HTTP page contains virus, the IAM gateway device will block this page. As to the virus file downloaded through HTTP or FTP, the IAM gateway device will influence the integrity of the file which cannot be opened. If the received email contains virus, the IAM gateway device will packet the file, label it as virus email and then send it to the receiver.

13.2. IPS

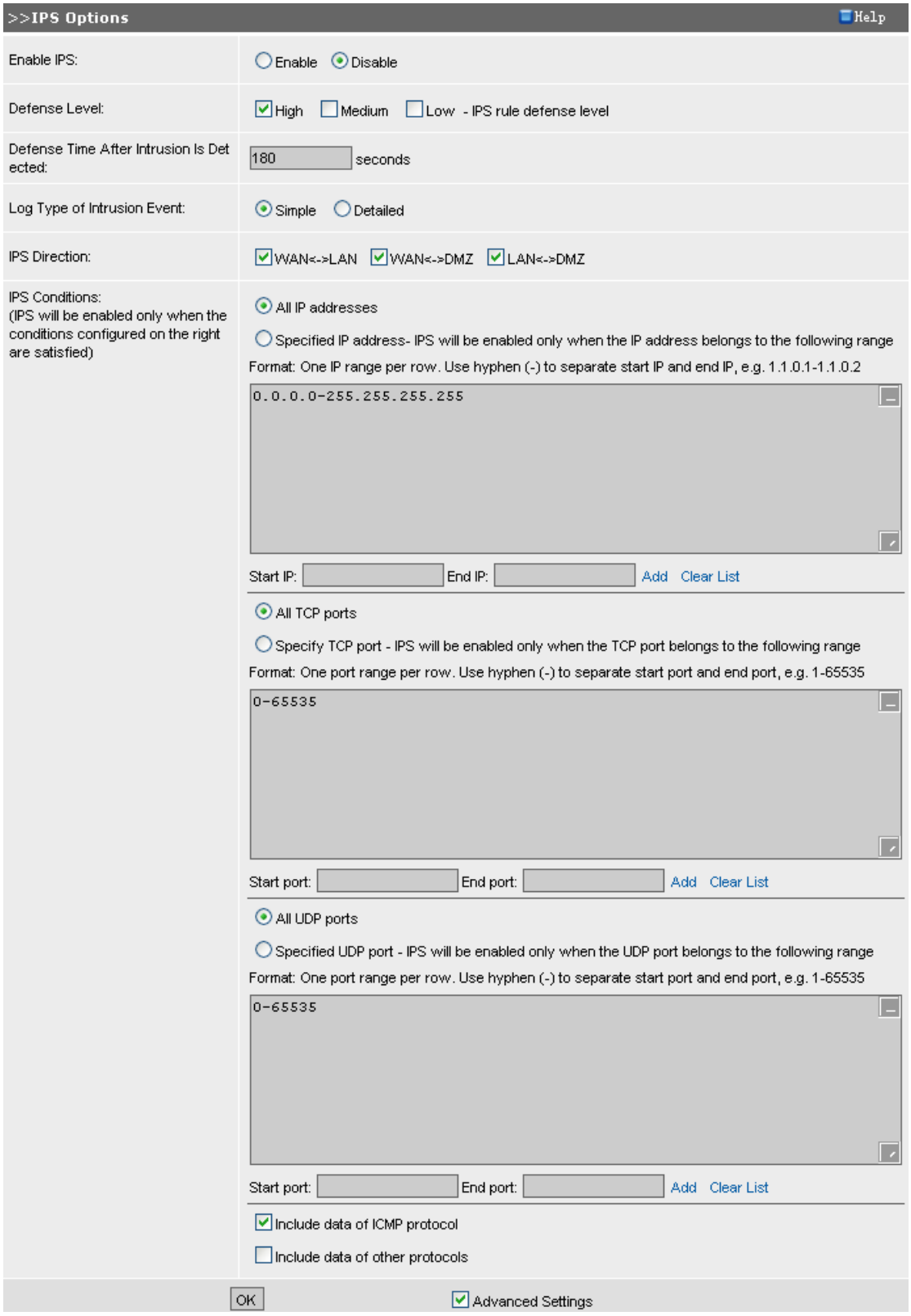
13.2.1. IPS Options

IPS (Intrusion Prevention System) can discover the potential risks that may be brought to the local area network (LAN) by detecting the data packets and analyzing its true use, and therefore decide whether to allow the data packets get into the local area network.

This section mainly introduces the parameters and the configuration of the intrusion protection system (IPS).

[Enable IPS]: Select [Enable] and click the <OK> button to enable the IPS function.

After enabling the IPS function, check the [Advanced Settings] option and configure the detailed parameters, as shown below:


>>IPS Options
Help
Enable IPS:
Enable
Disable
Defense Level:
High
Medium
Low - IPS rule defense level
Defense Time After Intrusion Is Detected:
180
seconds
Log Type of Intrusion Event:
Simple
Detailed
IPS Direction:
WAN<->LAN
WAN<->DMZ
LAN<->DMZ
IPS Conditions:
(IPS will be enabled only when the conditions configured on the right are satisfied)
All IP addresses
Specified IP address- IPS will be enabled only when the IP address belongs to the following range
Format: One IP range per row. Use hyphen (-) to separate start IP and end IP, e.g. 1.1.0.1-1.1.0.2
0.0.0.0-255.255.255.255
Start IP:
End IP:
Add
Clear List
All TCP ports
Specify TCP port - IPS will be enabled only when the TCP port belongs to the following range
Format: One port range per row. Use hyphen (-) to separate start port and end port, e.g. 1-65535
0-65535
Start port:
End port:
Add
Clear List
All UDP ports
Specified UDP port - IPS will be enabled only when the UDP port belongs to the following range
Format: One port range per row. Use hyphen (-) to separate start port and end port, e.g. 1-65535
0-65535
Start port:
End port:
Add
Clear List
Include data of ICMP protocol
Include data of other protocols
OK
Advanced Settings

[Defense Level]: There are three levels of defense rules provided by the SANGFOR IAM gateway device, [High], [Medium] and [Low]. Select a level according to the actual security need of your networking.

All the matching and suspicious attacks will be recorded by the IAM gateway device, and be handled according to the action configured for different defense levels.

As for the detailed logs, you can view then in the Data Center of the IAM gateway.

[Defense Time After Intrusion Is Detected]: Once attack attempt is detected, the IAM gateway device will defend against the attacker, denying all the data packets sent from this address in the next 180 seconds (default value). You can alter this value according to your case.

[Log Type of Intrusion Event]: Options are [Simple] (just record the general information of the intrusion and [Detailed] (record the data packets of the intrusion, which requires more storage capacity).

[IPS Conditions]: You can configure the options to defend the data transmission among WAN, LAN and DMZ zones against attacks according to your case. They are all enabled by default.

- Defense ability of [High], [Medium], and [Low] is in descending order. In general, it is recommended to check [High] which can ensure the security of the local area network and reduce the possibility of misjudgment.
- In almost all cases, the local area network is under the protection of the firewall of the IAM gateway device, and does not need the protection of IPS. In fact, the IPS is used for protecting the port with which the LAN server provides services to the external networks, in other words, it only maps the port to the local area network). This design can efficiently protect the local area network, and ensure the work efficiency of the IAM gateway device.

13.2.2. IPS Rules

[IPS Rules] enables you to view and configure the priority and auto update options of the IPS rules.

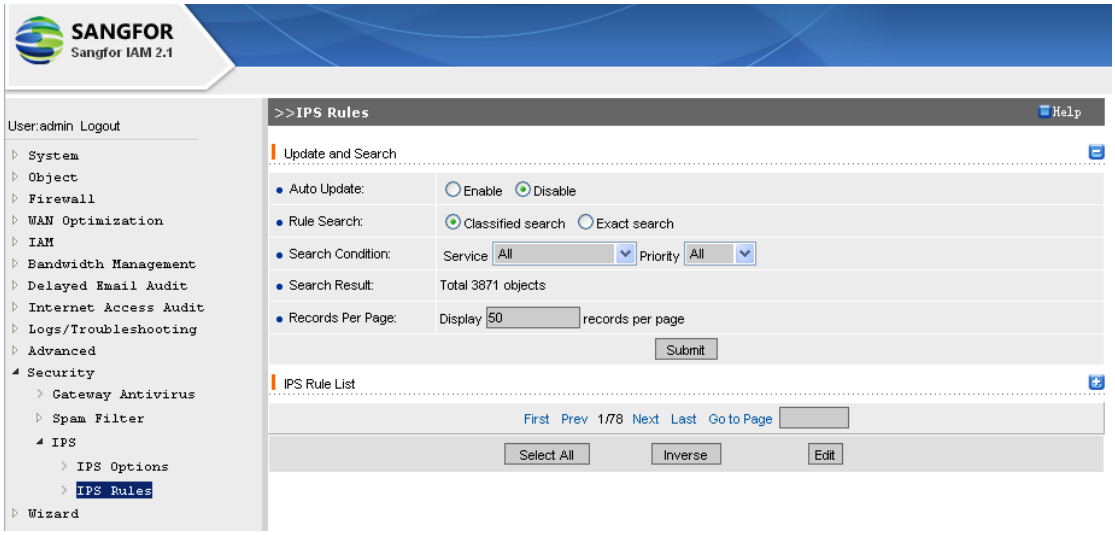
IPS rules can be arranged (viewed) according to service and priority. Priority of an IPS rule may be [High], [Medium]] and [Low].

[Auto Update]: Select [Enable] to allow the rules to be updated automatically.

[Rule Search]: To search for the existing rule(s), you can have [Classified search] and [Exact search].

<Detail>: Click it to view the detailed descriptions of the corresponding IPS rule.

If it happens that some legal and common applications are misjudged by the intrusion protection system, select a lower defense level. Procedures are: select a rule and click the <Edit> button to enter the [Edit IPS Rule] configuration page, as shown below:



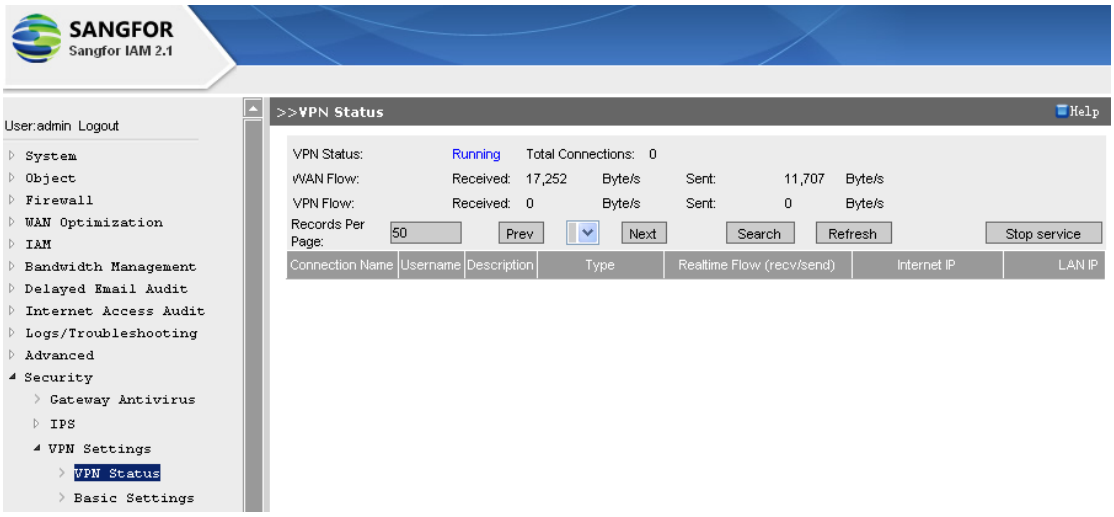
Alter the [Priority], selecting a lower level.

13.3. VPN Settings

13.3.1. VPN Status

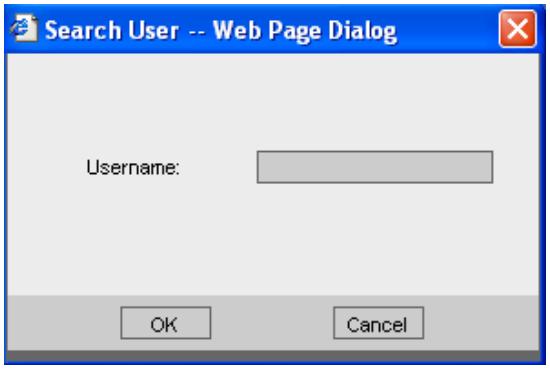
Click [VPN Setting] or [VPN status] to view the VPN connection and traffic information.

The page is as shown below:



<Search>: Click this button to open the [Search User] dialog; type the user name and click the <OK> button to quickly search for the connection information of this user.

The [Search User] dialog is as shown below:



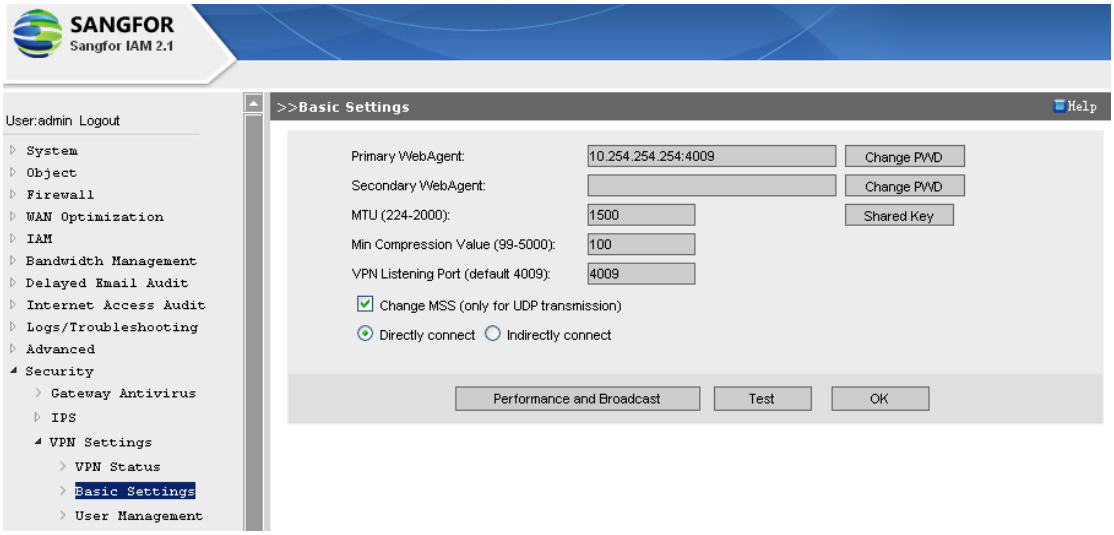
<Stop Service>: Click this button to stop the VPN service temporarily.

13.3.2. Basic Settings

[Basic Settings] covers the VPN-connection-related configurations, such as Webagent information, MTU, Minimum compression value, VPN listening port, VPN connection mode, broadcast and performance settings.

[Webagent]: The Webagent is the address (in the WEB server) where the dynamic IP addressing file is located.

The configuration page is as shown below:



[Primary WebAgent], [Secondary WebAgent]: If the VPN headquarters uses a dynamic IP address, enter a Webagent website (generally the website ends with ".pht"). You can click the <Test> button followed to check the connectivity of it; if the VPN headquarters uses a static IP address, the format is "IP address: port" (e.g., 202.96.134.133:4009).

Click the <Change PWD> button followed, and configure/modify the Webagent password, so as to prevent the illegal user from using the Webagent to masquerade the IP address.

Click the <Shared Key> to configure the shared key and prevent illegal device from connecting in.

- If it has multiple lines and the IP address(es) is static IP, the format of Webagent can be "IP1#IP2:port".
- If the Webagent password gets lost, there is no way to get back the lost password. The only solution is to contact the Customer Service of SANGFOR to generate a new file (without Webagent password) and replace the original one.
- If the [Shared Key] is configured, all the branch VPNs have to configure the same shared key to interconnect and communicate with each other.

[MTU]: Configures the MTU (Maximum Transmission Unit) of the data transmitted among the VPNs. It is 1500 by default.

[Min Compression Value]: Configures the minimum size of a VPN data packet that is to be compressed. It is 100 by default.

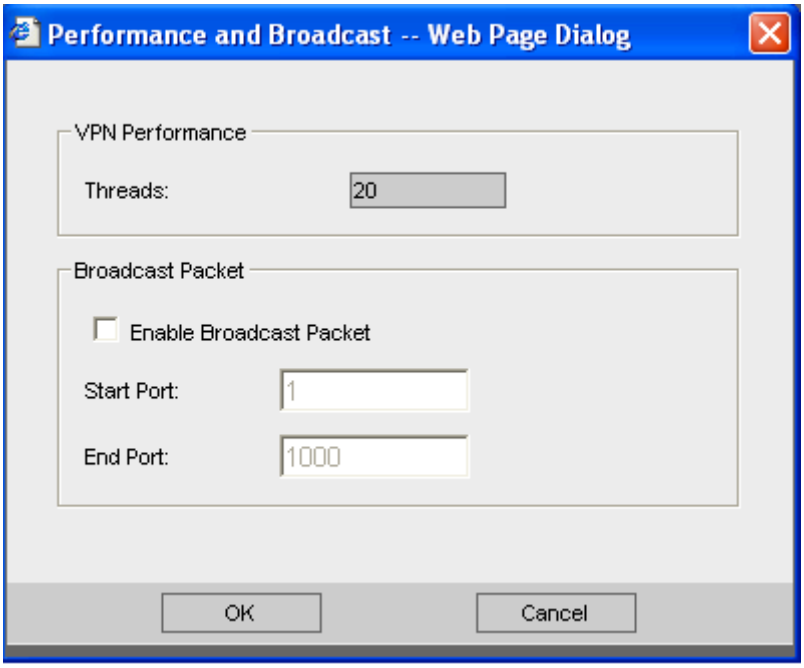
[VPN Listing Port]: Configures the listening port for the VPN service. If is 4009 by default. You can change the port according to your case.

[Change MSS]: Configures the maximum size of the fragmentation under UDP transmission.

[MTU], [Min Compression Value] and [Change MSS] are configured with the default values. If you need change the values, please follow the instructions given by the SANGFOR technicians.

[Directly connect], [Indirectly connect]: Select the connecting methods fulfilled between the IAM gateway device and the Internet, [Directly connect] or [Indirectly connect]. If the Internet IP address can be obtained directly or the Internet users can access the VPN port of the IAM gateway device with DNAT (destination translation) function, select [Directly connect]; if the Internet IP address cannot be obtained, select [Indirectly connect].

[Performance and Broadcast]: Configured the maximum number of VPN threads (connections) and whether to allow broadcast packets transmission among the VPN channels.



[Threads]: Configures the maximum number of VPN connections. It is 20 by default. One IAM gateway device allows maximum 1280 VPN connections. If you need to modify this parameter, please DO follow the instructions given by the SANGFOR technicians.

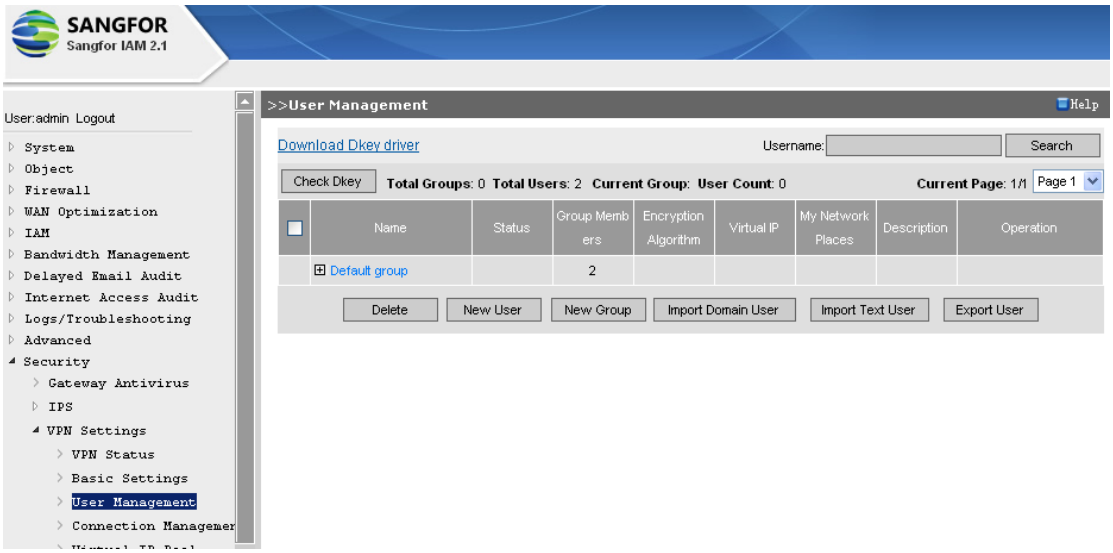
[Broadcast Packet]: Configures whether to allow broadcast packets transmission among the VPN

channels or not. You can specify a port to transmit broadcast packets, so as to avoid broadcast storm from appearing at the both ends of a VPN.

13.3.3. User Management

[User Management] is used for managing the connecting-in VPN accounts. The configurations include user account and password of the connecting-in VPN, the authentication method of the account verification, expiry date of the account, LAN privilege, group the user and the public attributes of the group users. Besides, it configures whether to enable hardware authentication, DKey and virtual IP.

The default configuration page is as shown below:



Click the <Check Dkey> button to inspect whether the DKey has inserted into the USB port of the computer (through which you have logged in to the IAM gateway console). If it has not yet installed the DKey driver, it will prompt to download the DKey driver.

Click the <Download DKey driver> link to download and install the driver.

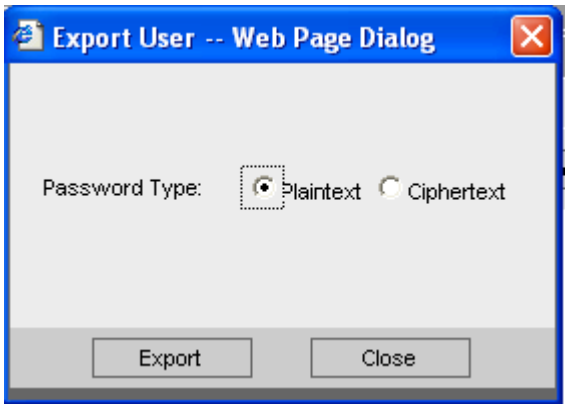
- Before generating the DKey, please DO install the DKey driver, otherwise the computer cannot recognize the DKey hardware.
- During the process of installing the DKey driver, please DO close the third-party anti-virus software and firewall, otherwise, conflicts between the programs will appear and the DKey

driver will fail to be installed.

<Delete>: Click this button to delete the selected user(s).

<Import Text User>, <Import Domain User>: Click this button to import the TXT or CSV file that contains the user information.

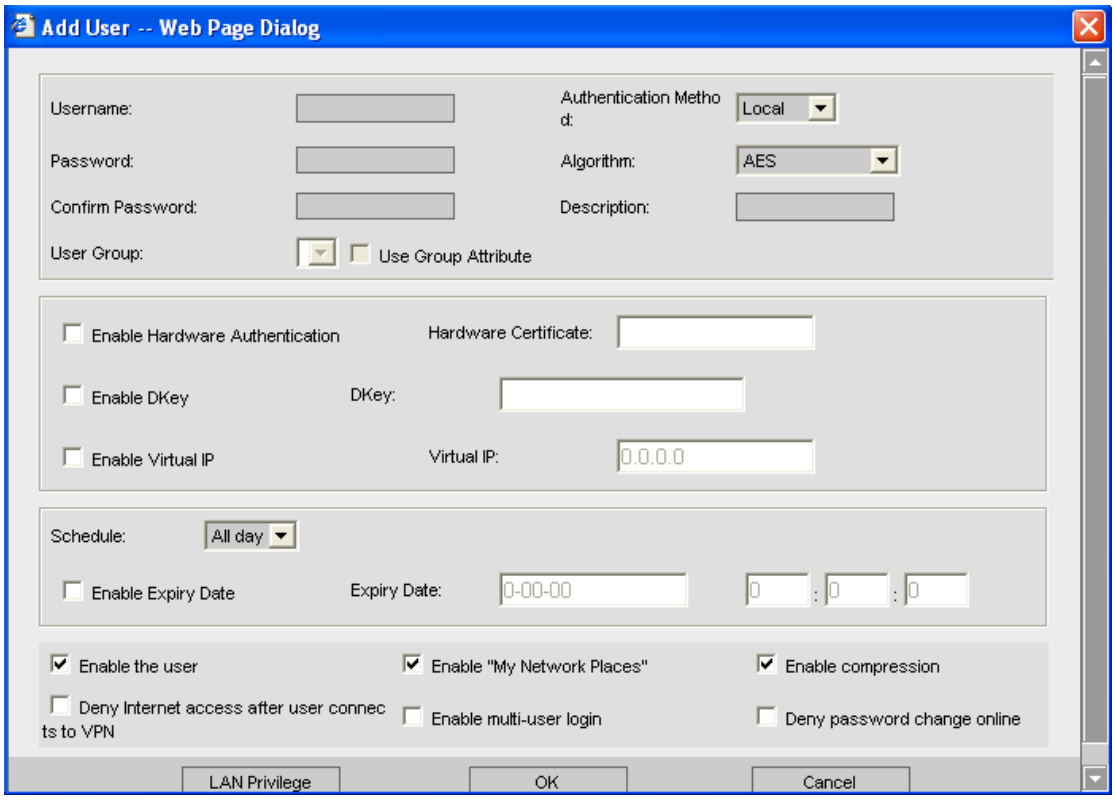
<Export User>: Click this button to export and save the users information of this IAM gateway device to the local computer. You can decide whether to export it as [Plaintext] or as [Cipher text]. The dialog is as shown below:



Click the <New Group> button to add a new user group. Type a name and description for this user group; define the group attributes (Encryption algorithm) and check [Enable 'My Network Places'] option. The dialog is as shown below:

Click <Add User> to add a new user. Configure the username, password, description and

algorithm, etc. The configuration dialog is as shown below:



[Authentication Method]: Configures the authentication method, [Local] (hardware authentication), [LDAP] or [RADIUS].

[Use Group Attribute]: Classifies the user into certain group and configures whether to have the user apply the group attributes.

- [User Group] is only available when there is a user group existing (please create user group first).
- If [Use Group Attribute] is checked, the [Algorithm], [Enable “My Network Places”] and [LAN Privilege] are unavailable.

[Enable Hardware Authentication]: Check this option to configure the hardware-featured certificate for authentication. Click the <Browse> button to select and upload the certificate file (in *.id format).

[Enable DKey]: Check this option to enable the mobile VPN user(s) to use DKey authentication.

Before enabling the DKey, please DO first insert the DKey into the USB interface of the computer and then generate the DKey.

[Enable Virtual IP]: Mainly is used for the connecting of the mobile VPN (users). If there are mobile VPN users, you have to check [Enable Virtual IP] option and configure a virtual IP address (LAN IP address in the virtual IP pool). Once a mobile VPN user connects to the VPN, it will take this allocated IP address as the virtual LAN IP. IP address 0.0.0.0 indicates that the system will automatically allocate a virtual LAN IP address (from the virtual IP pool) for this user.

[Schedule], [Enable Expiry Time]: Configures respectively the valid time and expiry time of the VPN user (connecting-in account).

[Enable "My Network Places"]: Check this option if the user of this VPN needs to use My Network Places.

[Enable compression]: Check this option and the IAM gateway device will compress the data to be transmitted between the IAM gateway device and the user, according to the selected algorithm.

This is a unique technology of SANGFOR VPN. It will take the best advantage of the bandwidth, in particularly in networking environment with limited bandwidth resources, and accelerate data transmission. However, this function is not suitable for all the cases. Check or uncheck this option according to your case.

[Deny Internet access after user connects to VPN]: This function is only available for the mobile VPN users. Check this option and the mobile VPN users can only visit the VPN device (headquarters) but cannot access the Internet.

[Enable multi-user login]: Check this option and this user account can be used by multiple users (for logon).

[Deny password change online]: Check this option and mobile VPN user cannot modify the login password after it connects to the VPN; uncheck this option and the user can modify the login password online.

[LAN Privilege]: Configures the privileges of this user after it connects to the VPN, such as the privileges of accessing some services. By default, there is not privilege limitation.

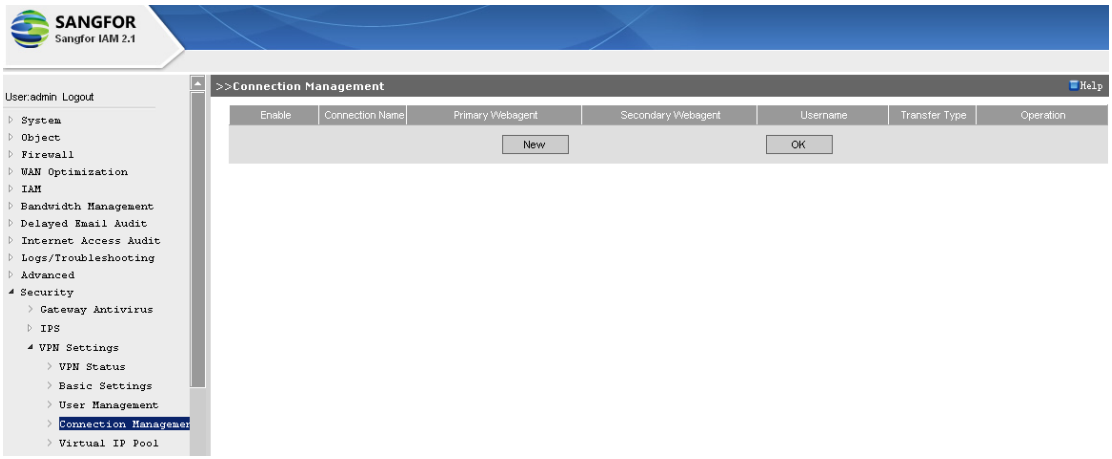
Before configuring [LAN Privilege], add some needed services in [VPN Settings] > [Advanced] > [LAN Service] page.

13.3.4. Connection Management

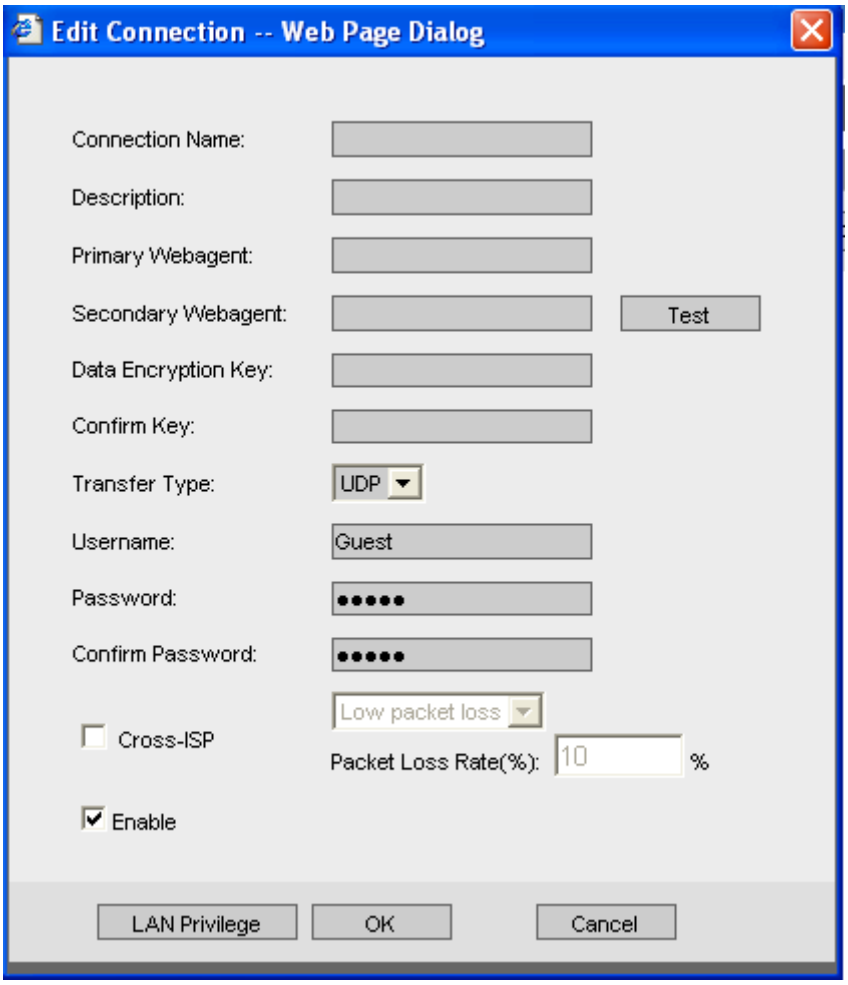
To enable it to realize interconnecting among multiple nodes and form a "Web-like" networking, the IAM gateway device offers the connection management function and configuration options to manage these nodes. These configurations are available in [Connection Management] page.

[Connection Management] function is only necessary when the local device need connect to other VPN devices as a Branch VPN. In other cases, that the local device is not a branch VPN of its peer, this function need not be enabled.

The [Connection Management] default configuration page is as shown below:



<New>: Click this button to add a new connection to the VPN headquarters. The configuration dialog is as shown below:



[Connection Name], [Description]: Type respectively the name and the description for this new connection.

[Primary Webagent], [Secondary Webagent]: Type the primary and secondary Webagent of the to-be-connected VPN headquarters. Click the <Test> button followed to check the availability of the Webagent. The testing results are as shown below:

- This test request is initiated by the local computer instead of the IAM gateway device.

- If the Webagent is a domain name, testing results show success and the webpage exists, otherwise, it indicates that the webpage does not exist. If the Webagent is a static IP address, testing results show success and the format (IP:PORT) of it is correct. In a word, successful testing results do not indicate connection success (of the VPN).

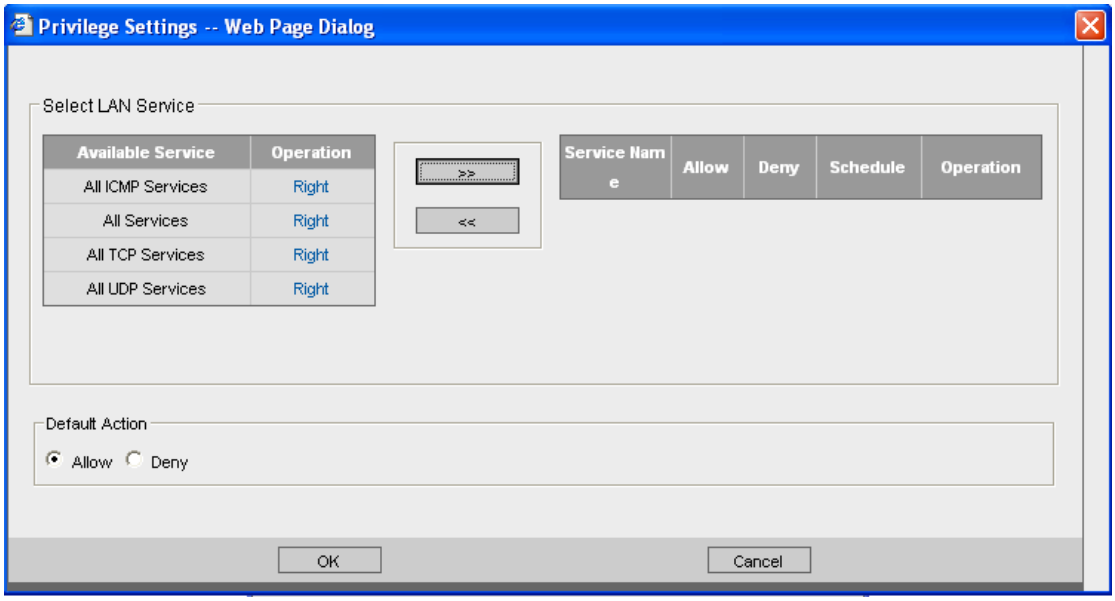
[Transfer Type]: Configures the transmission type of the VPN data packet. Options are “TCP” and “UDP”. It is UDP by default.

[Data Encryption Key], [Username] and [password]: Fill in the corresponding account information provided by the VPN headquarters.

[Cross-ISP]: If the VPN headquarters and the branch VPN apply different Internet service providers (ISP) and these different links cause frequent packet loss, this option is recommended to be checked. You can also configure the networking environment situation according to your case, [Low packet loss], [High packet loss] or [Set manually].

- To enable this function, you have to activate the cross-ISP license.
- Activate the cross-ISP license and check the [Cross-ISP] option, and then all the branch VPN users and mobile VPN users can gain the profits brought by the [cross-ISP] option when they are connecting to the VPN headquarters.

<LAN Privilege>: Click this button to enter the [Privilege Settings] configuration page and configure the privileges of the peer terminal, that is, to specify the services (provided by the local device) that will be available for the peer VPN connection.



Having completed configuring this page, you have to check [Enable] to activate this connection, and click the <OK> button to save all the settings.

13.3.5. Virtual IP Pool

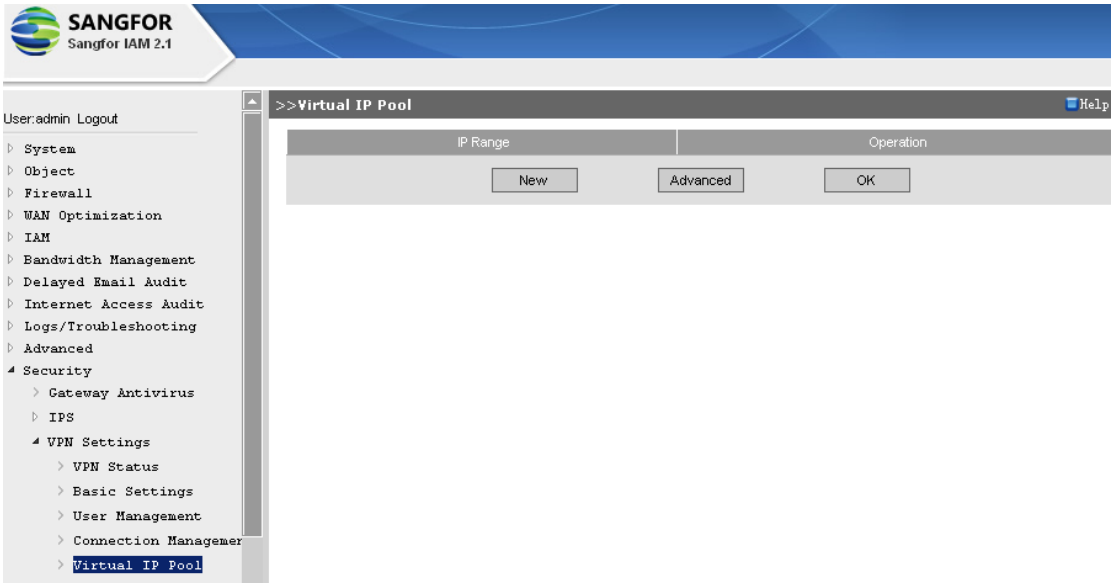
[Virtual IP Pool] contains the idle LAN IP addresses (or ranges) specified by the local SANGFOR IAM gateway device. These IP address are taken as the virtual IP addresses to be used by the mobile VPN users when they are getting connected to the gateway device (VPN).

When a mobile VPN user connects in, the IAM gateway device allocates a virtual IP address to this mobile VPN user. All the operations fulfilled by this mobile VPN user in the VPN headquarters are based on the allocated virtual IP address (source IP), completely the same with those fulfilled as a VPN headquarters LAN user. For instance, a mobile VPN user can visit any LAN computer of the VPN headquarters', though its computer does not direct its gateway to the IAM gateway device of the VPN headquarters; besides, you can configure some attributes for the mobile VPN user, such as DNS.

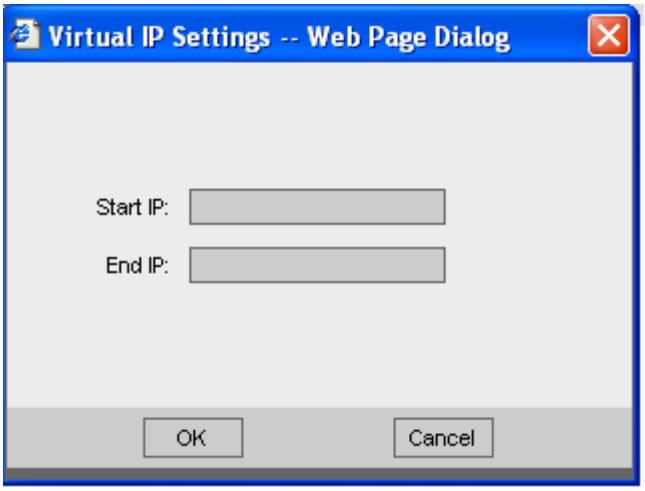
General procedures to configure a virtual IP address are as introduced below:

a). Create a virtual IP pool. The IP addresses (ranges) in this virtual IP pool should be idle ones of the local area network where the local SANGFOR IAM gateway device locates.

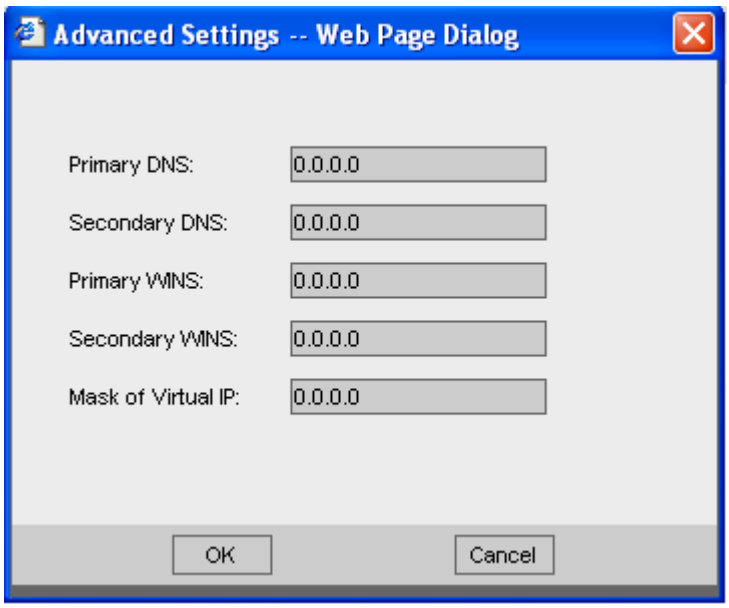
b). Allocate a virtual IP to a mobile VPN user. If the virtual IP is 0.0.0.0, the gateway device will automatically allocate a virtual IP address to this user. When the mobile VPN user connects in, the user will use the virtual IP address allocated or automatically allocated by the VPN headquarters (SANGFOR IAM gateway).



Click the <New> button to open the [Virtual IP Settings] configuration dialog; type the start IP and end IP. The dialog is as shown below:



Click the <Advanced> button to open the [Advanced Setting] configuration dialog; enter DNS, WINS server address, and the mask of virtual IP that is to be allocated to the virtual network adapter of the mobile VPN user. The configuration dialog is as shown below:

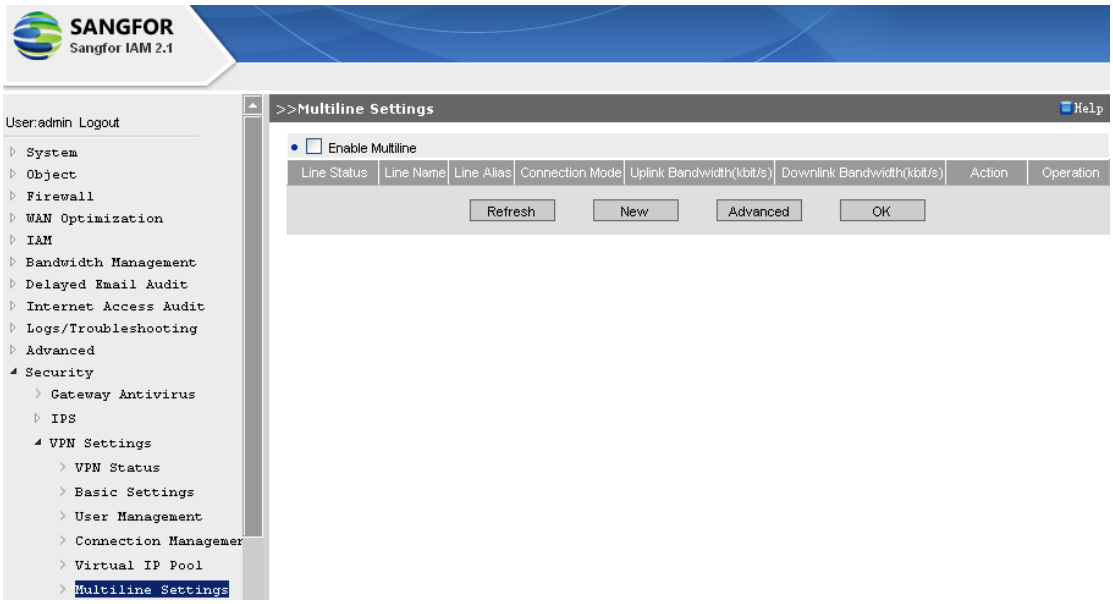


After configuring the [Advanced] options of the [Virtual IP Pool], the virtual network adapter of the mobile VPN user's computer must be configured as [Obtain an IP address automatically] and [Use the following DNS server addresses], otherwise, the addresses configured in [Advanced] will not be allocated to the virtual network adapter of the mobile VPN user's computer.

13.3.6. Multiline Settings

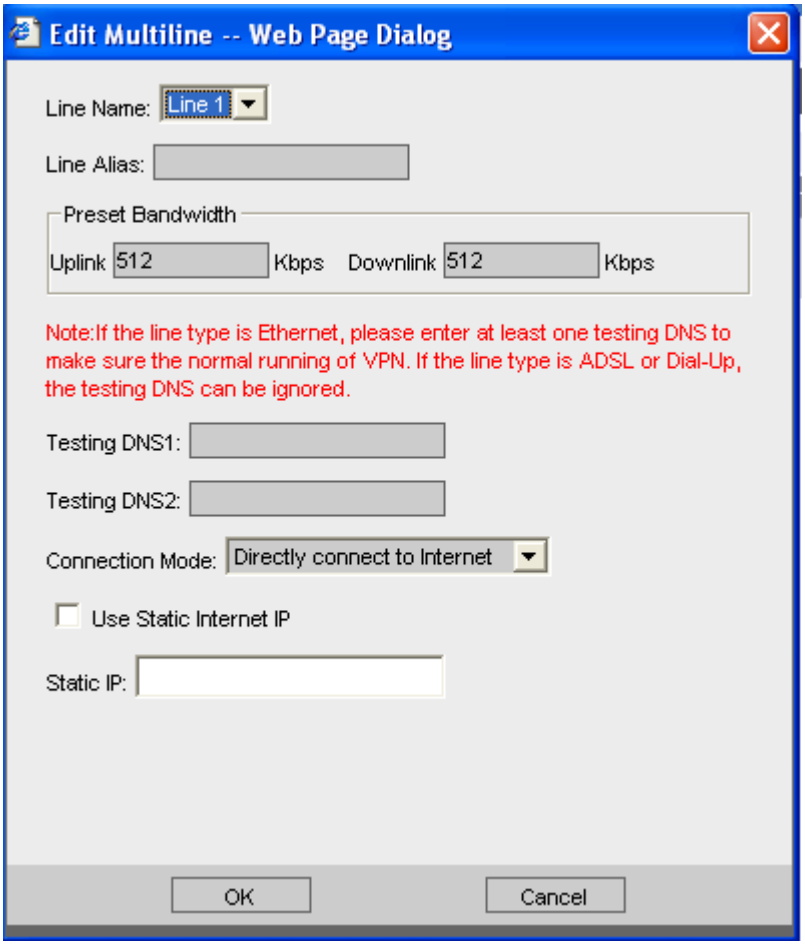
When there are multiple external lines, the [Multiline Setting] must be configured. You can add or delete a line here, or modify the line selection policy.

The [Multiline Settings] default configuration page is as shown below:



If your networking has multiple lines connecting to the external network, check [Enable Multiline] and then add the line.

Click the <New> button to enter the [Edit Multiline] page and add a new line; the configuration dialog is as shown below:

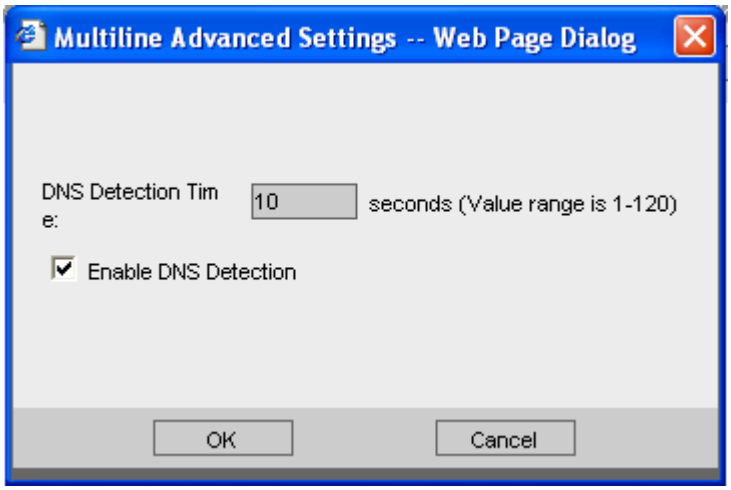


Select a line and name it; configure the [Preset Bandwidth] and [Connection Mode] according to the actual information of the line; and then click the <OK> button to complete configuring this line.

[Static IP]: If the interface IP address is a static IP address, type it in this text box; if it is a dynamic IP address, leave this text box blank.

- If it is an Ethernet line, you have to configure the testing DNS which is working for the Internet. If it is an ADSL or Dial-up line, the [Testing DNS] can be left blank.
- As to the [Preset Bandwidth], the uplink and downlink bandwidth must be coherent to the actual bandwidth.

Under the default configuration page, click the <Advanced> button to open the [Multiline Advanced Settings] configuration dialog, as shown below:



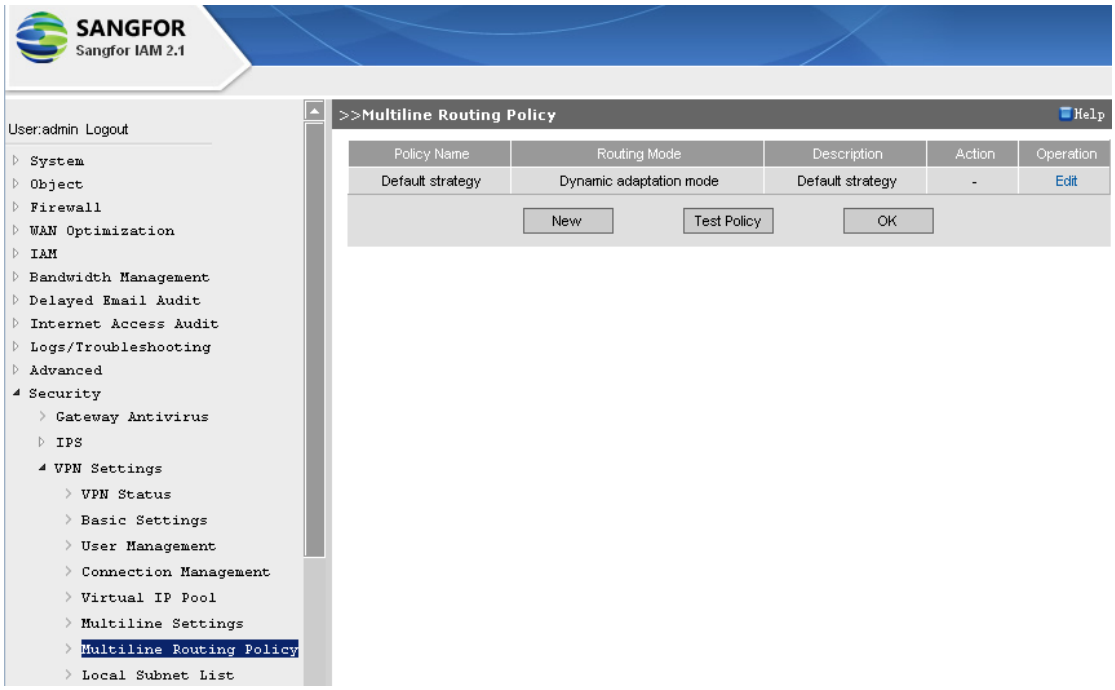
Check [Enable DNS Detection] to enable it to detect the status of the multiple lines.

[DNS Detection Time]: Configures the time interval of fulfilling DNS detection. Only when the [Enable DNS Detection] option is checked will the settings take effect.

13.3.7. Multiline Routing Policy

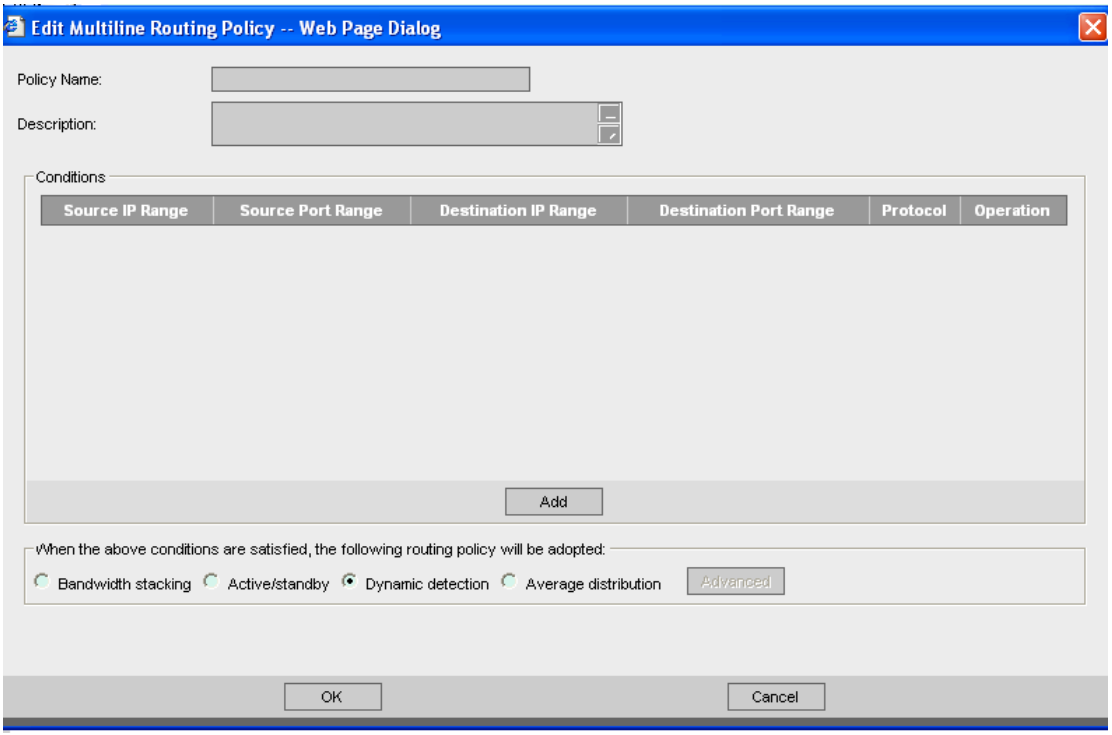
SANGFOR IAM gateway device offers the powerful multiline routing policy for VPN. You can

configure the multiline policy to achieve intercommunication among different VPNs, according to the protocol applied, source IP, destination IP, source port, destination port, etc.

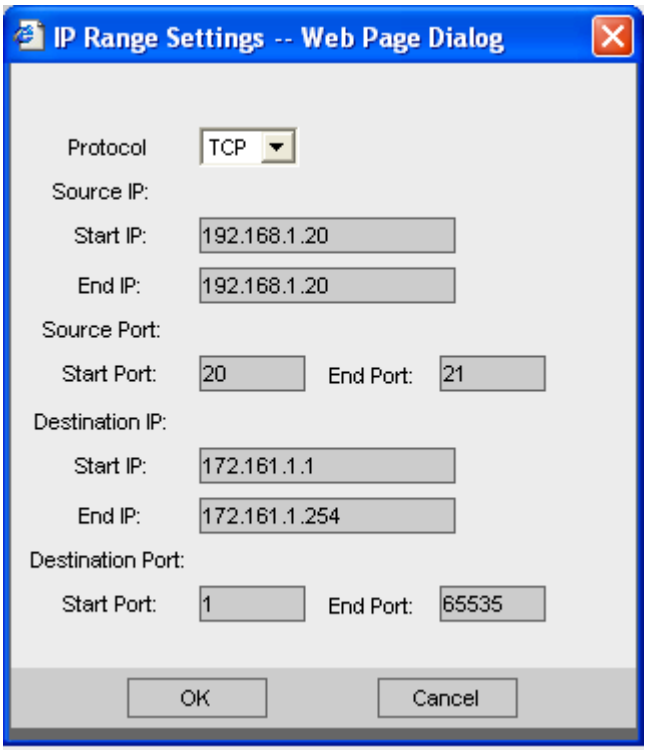


For example, the Branch1 (172.16.1.0/24) need visit the FTP server (IP: 192.168.1.20) of its headquarters. We are to configure a multiline routing policy, so as to have the data packets from Branch1 transmitted to the FTP server through Line 1.

Under the [Multiline Routing Policy] default configuration page, click the <New> button to enter the [Edit Multiline Routing Policy] page, as shown below:



Click the <Add> button to enter the [IP Range Settings] configuration dialog; configure the IP addressed and ports, and select a protocol, as shown below:



[Protocol]: Select a protocol for data transmission. In this example, it is TCP.

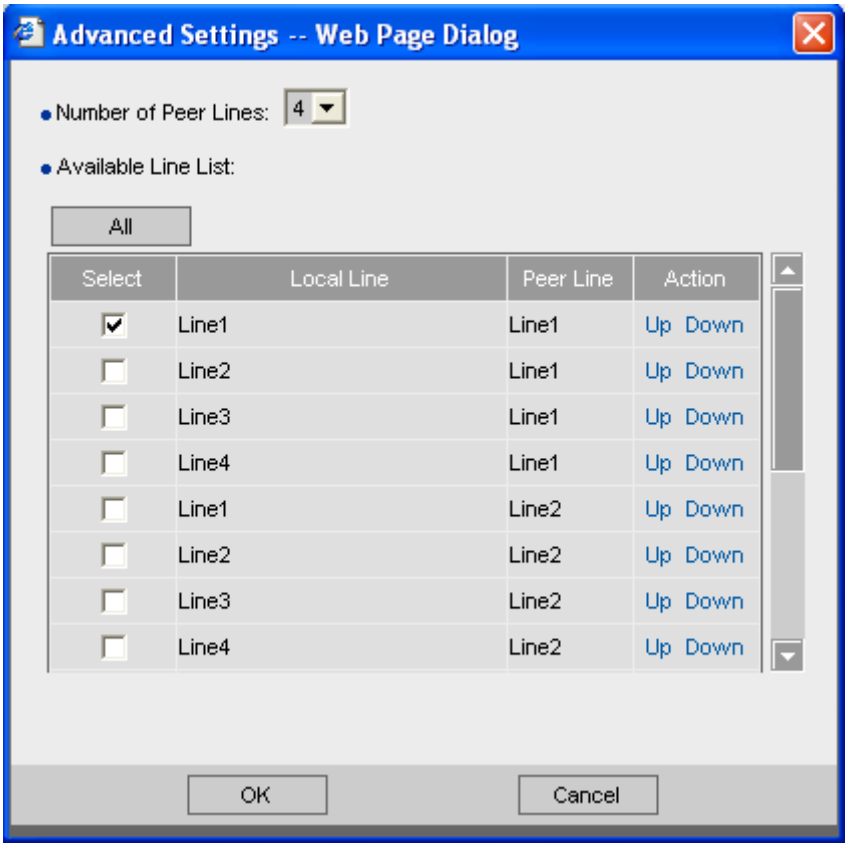
[Source IP]: Type a LAN IP address (of the local-terminal segment). In this example, it is 192.168.1.20.

[Source Port]: Type a service port (of the local-terminal segment). In this example it is 20-21.

[Destination IP]: Type an IP address (or the peer-VPN segment. In this example, it is the LAN IP range of the Branch1, 172.16.1.1-172.16.1.254.

[Destination Port]: Type a port through which the peer VPN (Branch1) is to visit the services (provided by the local terminal). In this example, it is 1-65535, all the ports.

Under the [Edit Multiline Routing Policy] page, select [Bandwidth stacking] and check the <Advanced> button to enter the [Advanced Settings] page, as shown below:



Select the needed line for data transmission. In this example, it is from local line [Line 1] to peer line [Line 1]. After that, click the <OK> button to save the settings.

- In the above example, Branch1 has only one line connecting to its VPN headquarters. If the branch has several lines connecting to the headquarters, you can select [Number of Peer Lines] and select the needed lines in the list.
- The [Advanced Settings] is only available for [Bandwidth stacking], [Active/standby] and

[Average distribution] routing policy options.

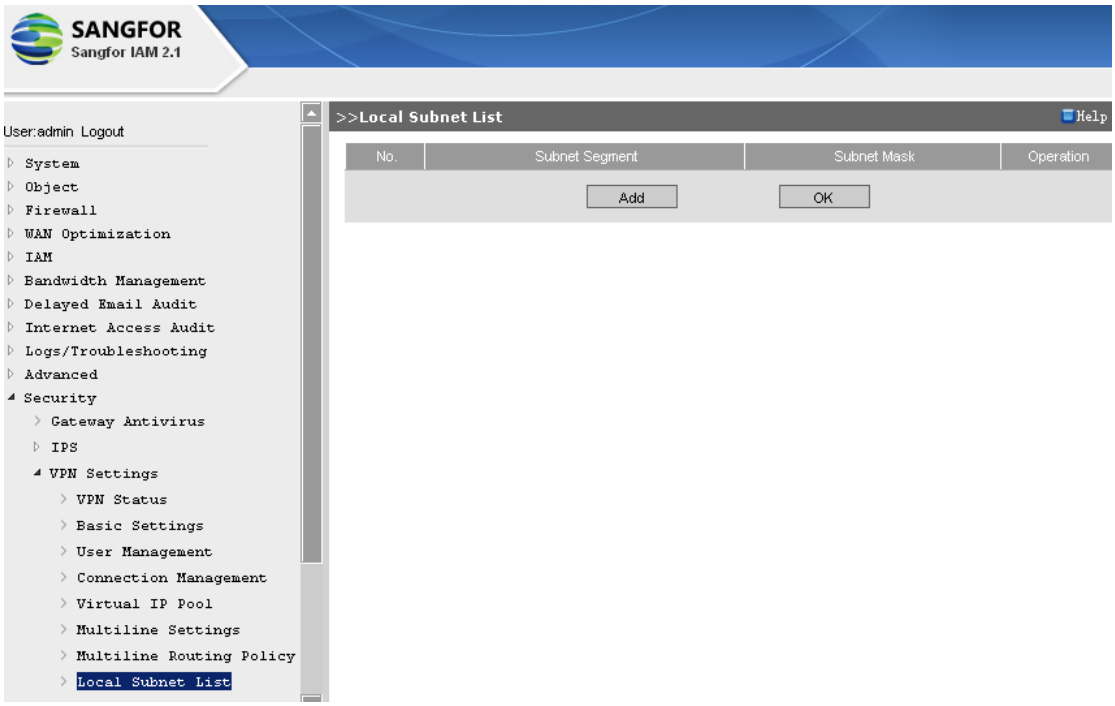
- If the routing policy selected is [Dynamic detection] option, the system will choose a line (an optimal line) for the fastest connection). If policy-selected line is in fault, the system will automatically switch to an available line to ensure the smooth transmission of the data.

13.3.8. Local Subnet List

[Local Subnet List] functions when there are multiple subnets existing in the local area network of the IAM gateway device, and the branch VPN users also need to visit other subnets of this network (the VPN headquarters).

For example, there are two subnets (192.200.100.x and 192.200.200.x). We are to configure the [Local Subnet List] to enable the branch VPN, mobile VPN, and VPN headquarters to interconnect with each other. The detailed steps are as shown below:

Step 1: Configure the related subnets in the [Local Subnet List]. The configuration page is as shown below:



[Subnet Segment], [Subnet Mask]: Configures the network ID of the other LAN and subnet mask.

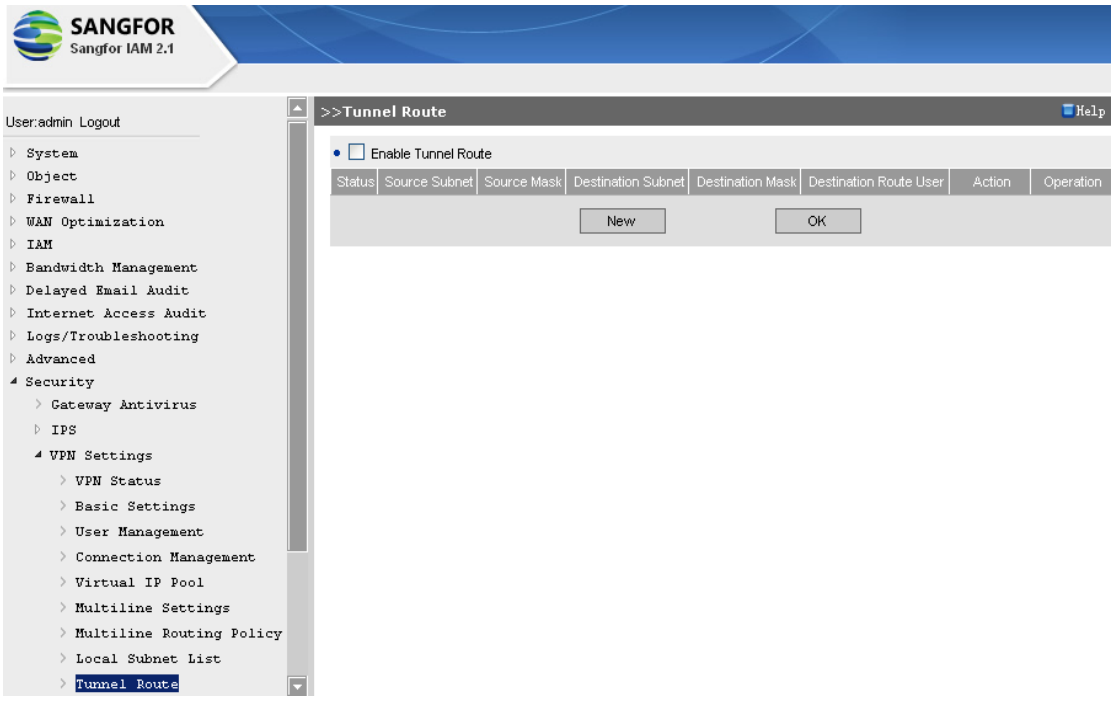
Step 2: Configure the route for the related subnets in the [Static Routing] page. For detailed configuration page, please refer to Section 3.14.2 Static Routing.

The [Local Subnet List] stands for a kind of “declaration”. The subnets defined here will be regarded as VPN segments by the VPN device and the client-end software. All the data going through the VPN device or software will be encapsulated and transmitted through the VPN tunnels. Therefore, you need to configure the [Static Route], in addition to adding the related subnets into the [Local Subnet List]], so as to enable the intercommunication among these subnets.

13.3.9. Tunnel Route

SANGFOR IAM gateway device offers the powerful VPN tunnel route configuration function. You can configure route for the VPN tunnels, to achieve interconnection among different VPNs (software/hardware) and establish a true web-like VPN network.

The [Tunnel Route] default configuration page is as shown below:



For example, the Shenzhen headquarters (192.168.1.x/24) needs to establish VPN connection with its branches Shanghai (172.16.1.x/24) and Guangzhou (10.1.1.x/24); however, there is no VPN tunnel between the Shanghai branch and Guangzhou branch. To achieve interconnection between the two, we are to configure a tunnel route. The detailed configuration is as shown below:

Step 1: Configure [Tunnel Route] on the Shanghai branch’s IAM gateway device. Check [Enable Tunnel Route] and click the <New> button to add a route directing to the Guangzhou branch, as

shown below:

[Source Subnet]: Configures the network ID of the source subnet. In this example, it is 172.16.1.0.

[Source Mask]: Configures the mask of the source subnet. In this example, it is 255.255.255.0.

[Destination Subnet]: Configures the network ID of the destination subnet. In this example, it is 10.1.1.0.

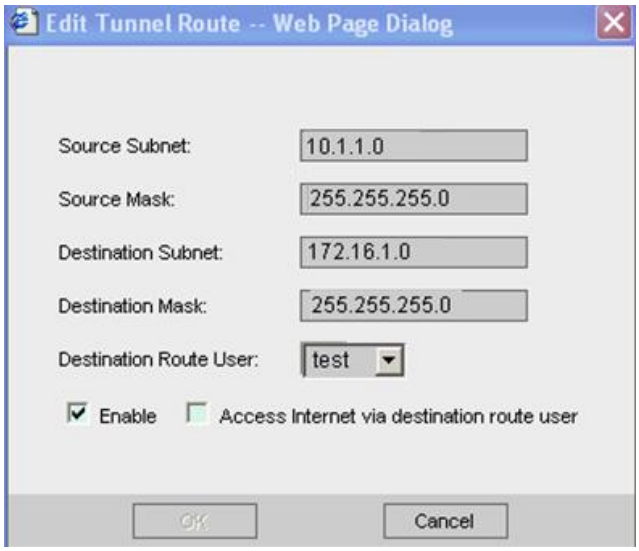
[Destination Mask]: Configures the mask of the destination subnet. In this example, it is 255.255.255.0.

[Destination Route User]: Refers to the user that is used to establish the VPN connection with the headquarters, that is, the user selected in the [VPN Settings] > [Connection Management] > [Edit Connection] configuration dialog. It determines the VPN device to which the packets are forwarded. In this example, it is Guest (Shanghai).

- [Source Subnet] and [Destination Subnet] define respectively the source IP address and destination IP address of the data to be transmitted. If the data packet satisfies these two conditions, this route will take effect, and the data will then be transmitted to the corresponding VPN device.
- [Destination route user] determines the VPN device to which the data packets are forwarded

by this tunnel route (indicating the corresponding username selected in the [VPN Settings] > [Connection Management] > [Edit Connection] configuration dialog. In this example, the branch Shanghai has established a VPN connection with its headquarters (using the name "Guest" in the [Connection Management] configuration page). Therefore, we choose the [Destination Route User] "Guest" as the route to forward the data to its headquarters' VPN device.

Step 2: Configure [Tunnel Route] on the Guangzhou branch's IAM gateway device. Check [Enable Tunnel Route] and click the <New> button to add a route directing to the Shanghai branch, as shown below:



[Source Subnet]: Configures the network ID of the source subnet. In this example, it is 10.1.1.0.

[Source Mask]: Configures the mask of the source subnet. In this example, it is 255.255.255.0.

[Destination Subnet]: Configures the network ID of the destination subnet. In this example, it is 172.16.1.0.

[Destination Mask]: Configures the mask of the destination subnet. In this example, it is 255.255.255.0.

[Destination Route User]: Configures the VPN device to which this tunnel route directs (indicating the corresponding username selected in the [VPN Settings] > [Connection Management] > [Edit Connection] configuration dialog). In this example, it is test (Guangzhou).

The tunnel route also is used for forwarding all the Internet access requests of a branch user to its VPN headquarters, enabling the branch VPN user to get access to the Internet through the VPN headquarters' WAN interface. The configuration is as shown below:

[Source Subnet]: Configures the network ID of the source subnet which needs to connect to the Internet through the VPN headquarters. In this example, it is 172.16.1.0 (Shanghai branch).

[Source Mask]: Configures the mask of the source subnet. In this example, it is 255.255.255.0.

[Destination Route User]: Configures the VPN device to which this tunnel route directs (indicating the corresponding username selected in the [VPN Settings] > [Connection Management] > [Edit Connection] configuration dialog). In this example, it is Guest (Shanghai).

Finally, check the [Access Internet via Destination Route User] option and click <OK> button to activate the above settings.

If the VPN headquarters device is configured as and deployed in Route mode, you have configure a corresponding SNAT rule for the VPN segment in the [Firewall] > [NAT Rules] > [SNAT] configuration page. For detailed configuration guide, please refer Section 5.2.1 SNAT.

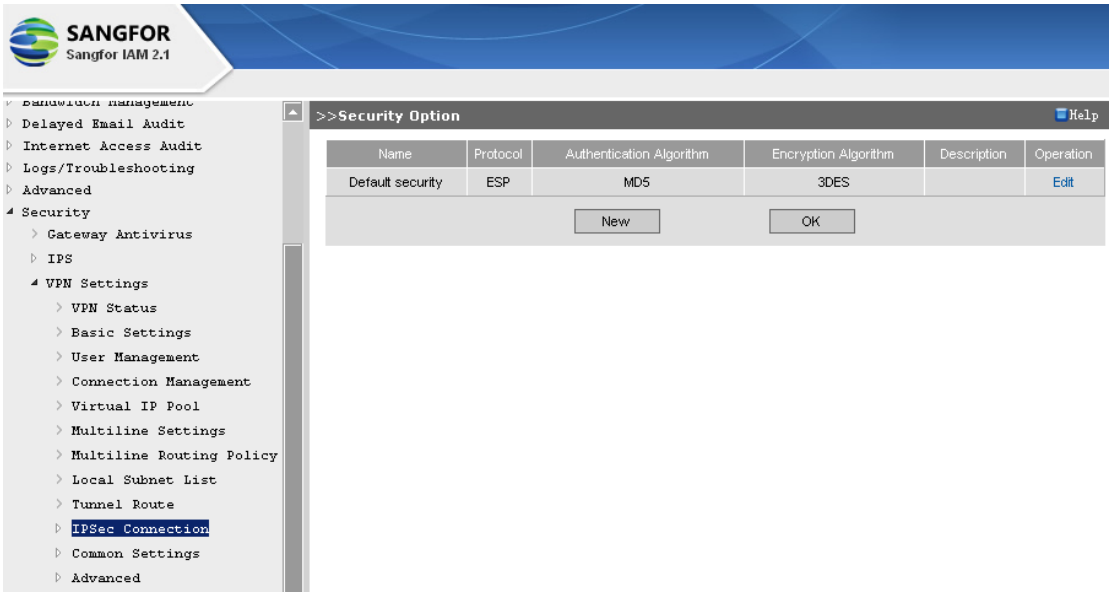
13.3.10. IPSec Connection

SANGFOR IAM gateway can connect with a third-party VPN device to establish standard IPSec VPN connection.

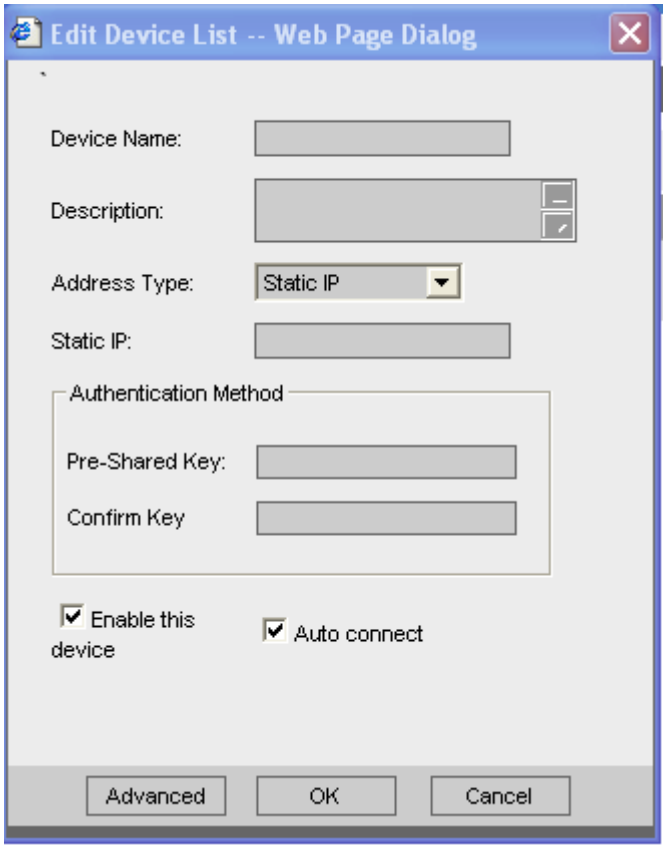
13.3.10.1. Device List

[Device List] can enable the SANGFOR IAM gateway device to connect with a peer VPN to establish a standard IPSec connection. It is the first phase of negotiation of the standard VPN protocol.

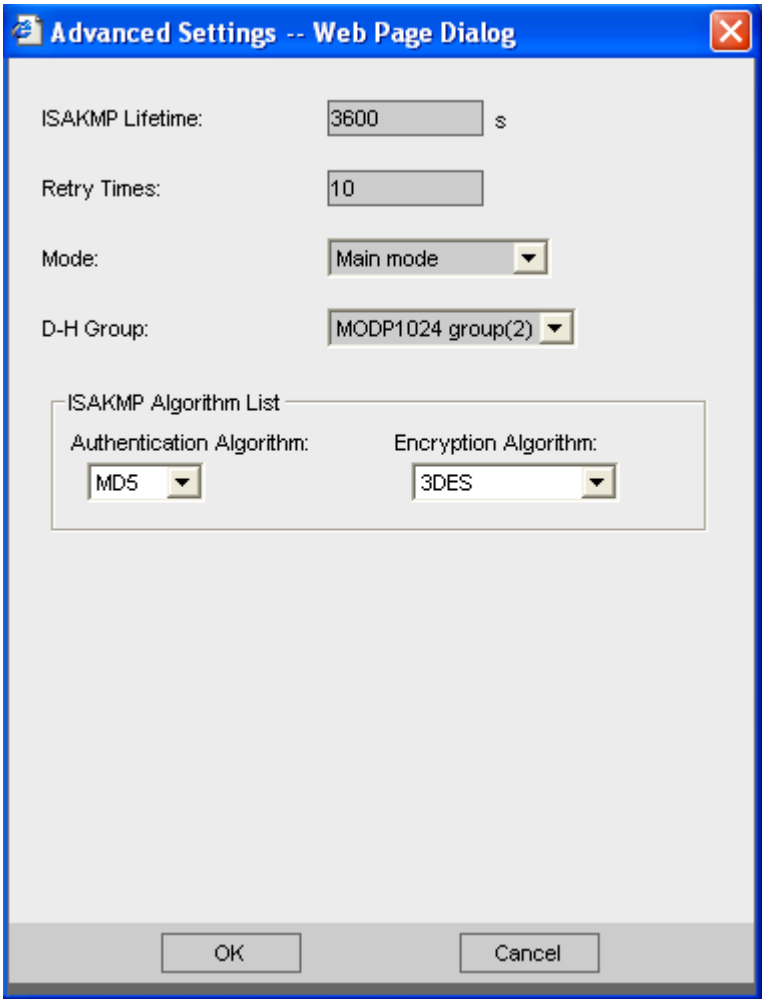
The default configuration page is [Device List] is as shown below:



Select an [Outlet Line] and click the <New> button. An [Edit Device List] configuration page pops up, as shown below:



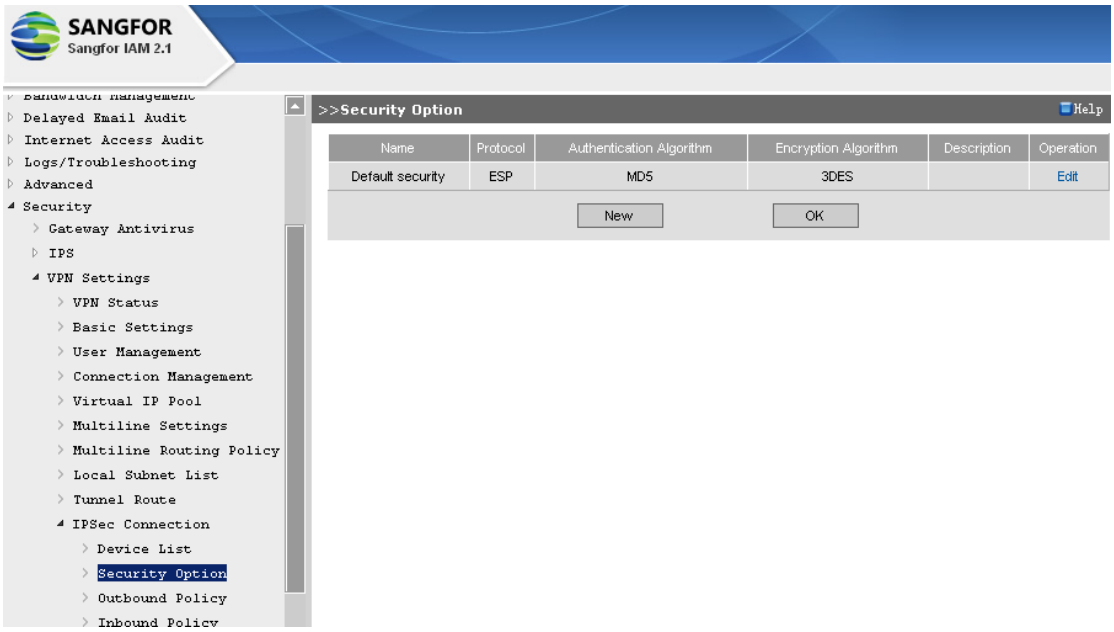
Click the <Advanced> button to view the advanced settings. The configuration dialog is as shown below:



13.3.10.2. Security Option

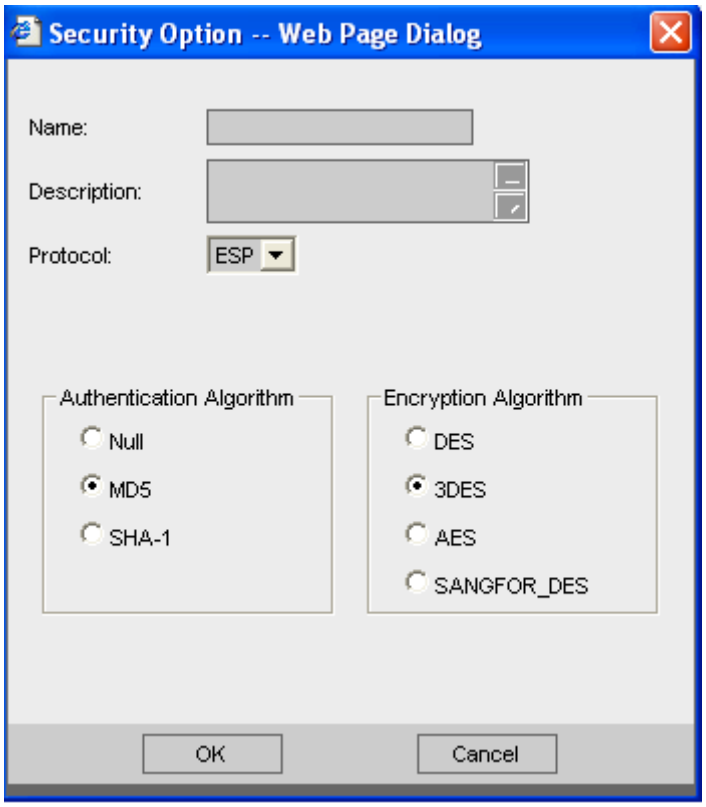
[Security Option] configures the parameters used for establishing standard IPSec connection. This is the second phase of IPSec negotiation.

The configuration page is as shown below:



Before establishing IPSec connection with a third-party, first configures the policy to be used by the peer device. The policy includes the rules of [Protocol] (AH or ESP), [Authentication Algorithm] (MD5 or SHA-1) and [Encryption Algorithm] (DES, 3DES or AES).

Click the <New> button and the [Security Option] appears, as shown below:



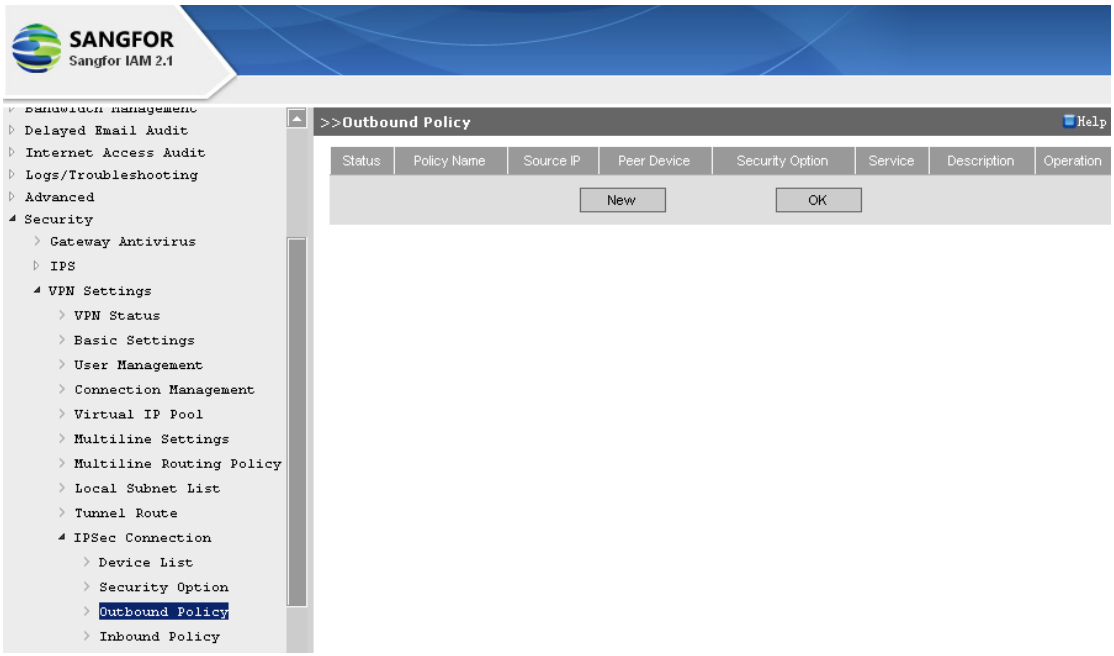
SANGFOR IAM gateway device will negotiate and establish IPSec connection with the peer device according to the configured policy.

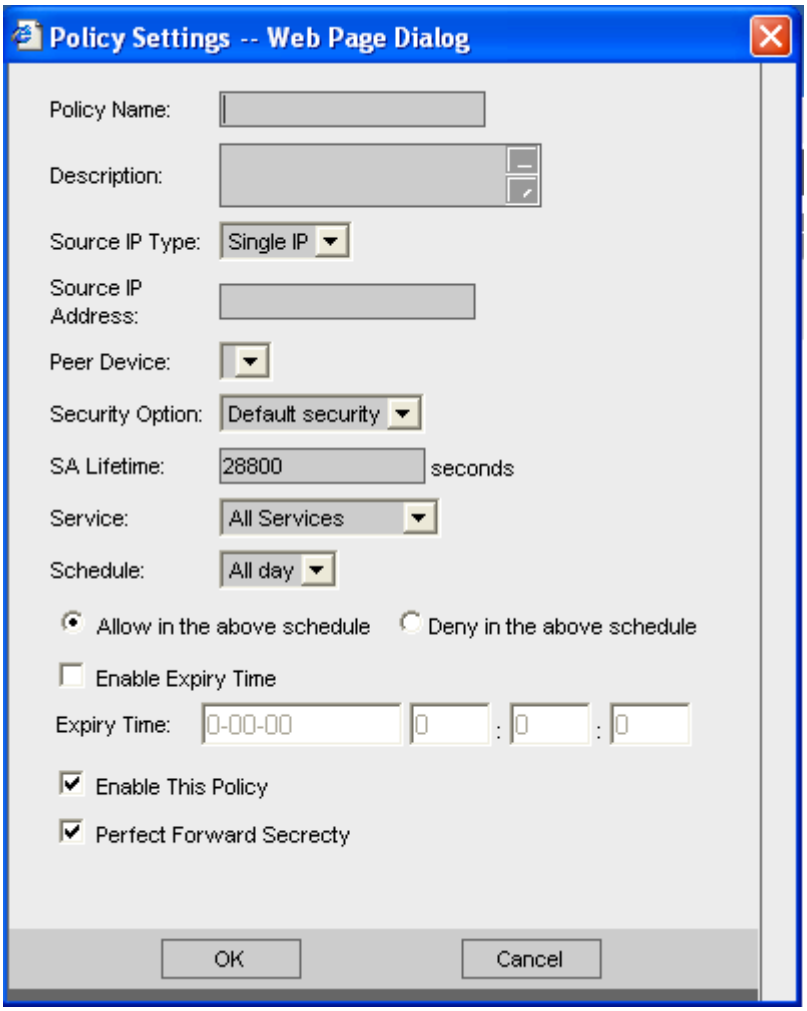
The [Encryption Algorithm] functions during the second Phase of IPSec connection. If there are multiple devices interconnected and each applies a different policy, you then have to add the policy of each device to the security potion list (i.e., create the corresponding policy for each device).

13.3.10.3. Outbound Policy

[Outbound Policy] configures the rule used for the data packets transmission from the local device to the peer device.

Click the <New> button and the [Policy Settings] appear, as shown below:

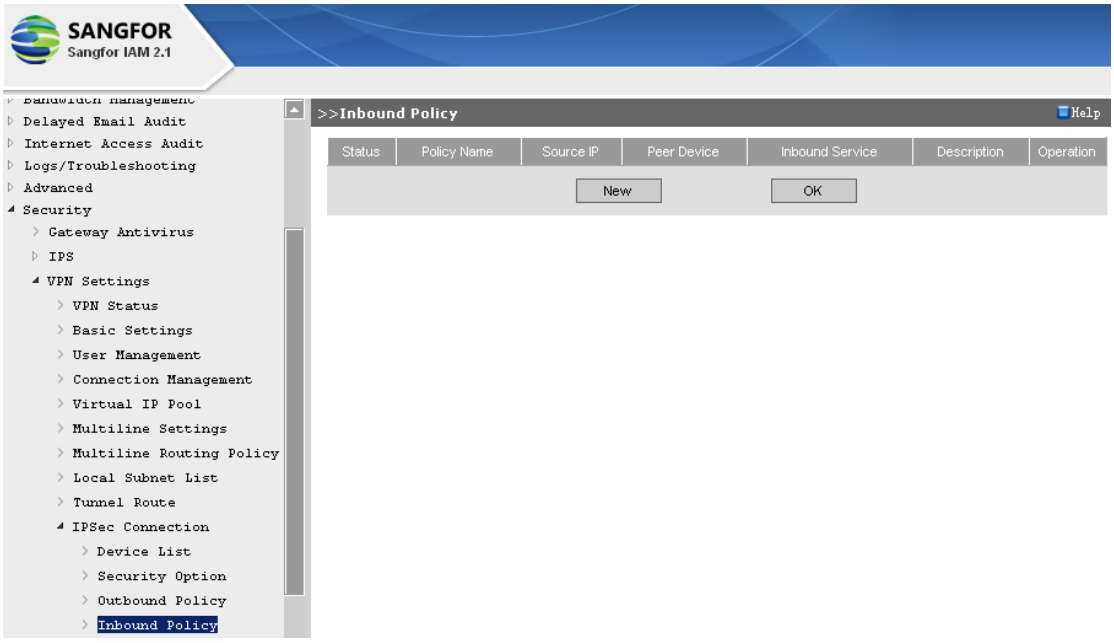


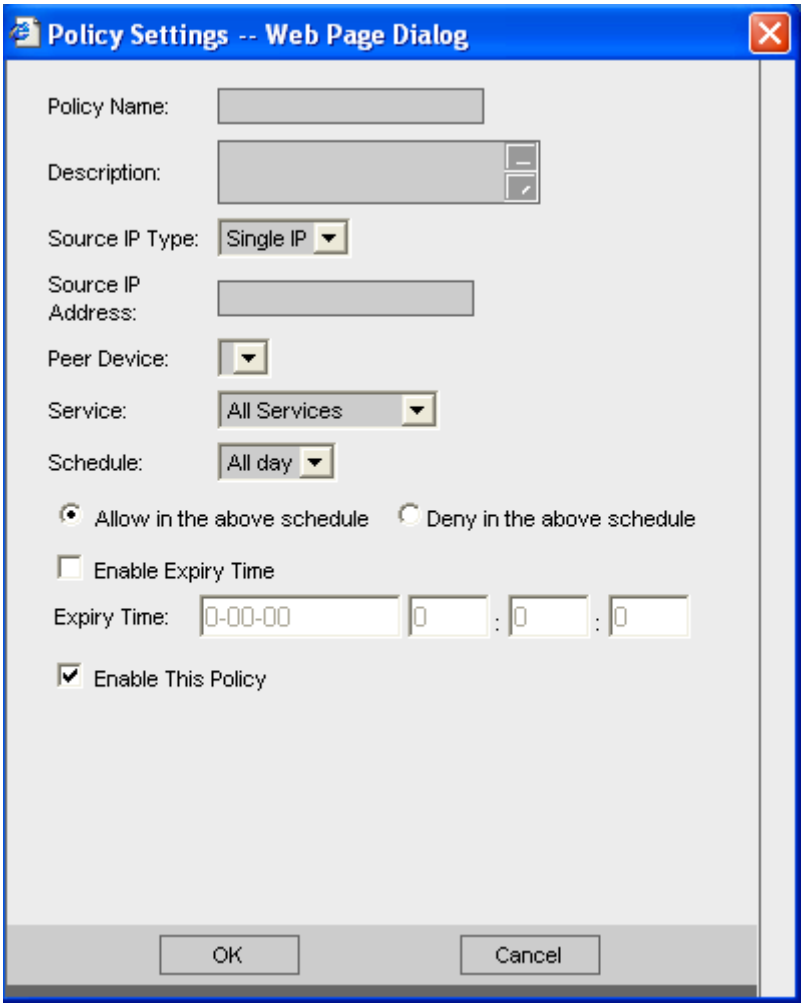


13.3.10.4. Inbound Policy

[Inbound Policy] configures the rule used for data transmission from the peer device to the local device.

Click the <New> button and the corresponding [Policy Settings] appears, as shown below:


SANGFOR
Sangfor IAM 2.1
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Security
Gateway Antivirus
IPS
VPN Settings
VPN Status
Basic Settings
User Management
Connection Management
Virtual IP Pool
Multiline Settings
Multiline Routing Policy
Local Subnet List
Tunnel Route
IPSec Connection
Device List
Security Option
Outbound Policy
Inbound Policy
>>Inbound Policy
Help
Status
Policy Name
Source IP
Peer Device
Inbound Service
Description
Operation
New
OK


Policy Settings -- Web Page Dialog
Policy Name:
Description:
Source IP Type:
Single IP
Source IP Address:
Peer Device:
Service:
All Services
Schedule:
All day
Allow in the above schedule
Deny in the above schedule
Enable Expiry Time
Expiry Time:
0-00-00
Enable This Policy
OK
Cancel

- Both the [Service] and [Schedule] of [Outbound Policy]/[Inbound Policy] are extra rules provided by the SANGFOR IAM gateway device, and only take effect on the local device, which means, these rules are not the negotiation topics during the process of negotiating with the third party and establishing the VPN connection.
- The eventual source address(es) applicable to the [Outbound Policy] and [Inbound Policy] refers to the source IP addresses allowed to connect in/out by the local VPN device are those that are included in both the [Source IP] configured in the inbound/outbound policy and the [Source IP Range] referenced by the selected LAN service.

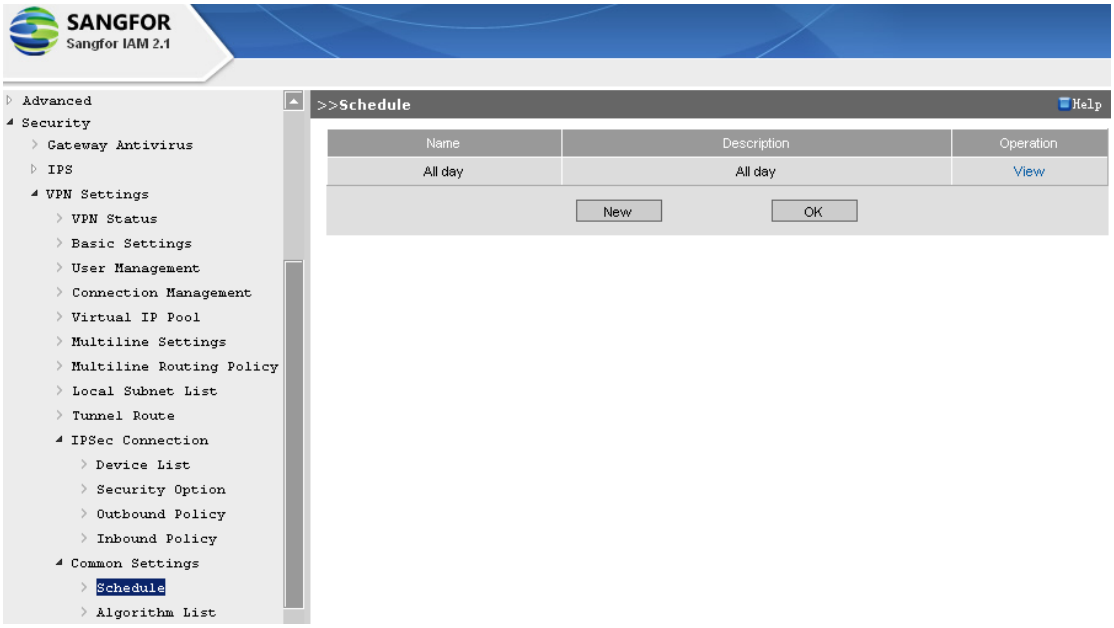
13.3.11. Common Settings

[Common Settings] covers the configuration of [Schedule] and [Algorithm] modules.

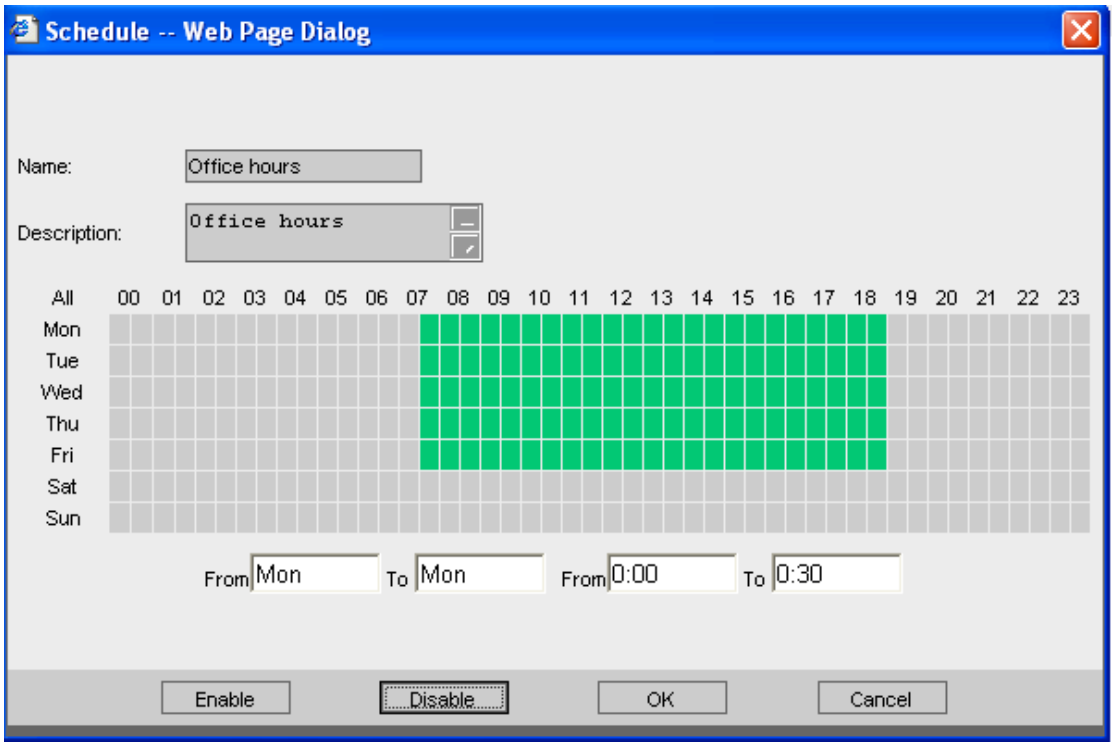
13.3.11.1. Schedule

[Schedule] defines the commonly used time periods, mainly used as valid time or expiry time. The schedule can be referenced by [User Management] and [LAN Privilege] configurations. The time is the same with the system time of the IAM gateway device.

The [Schedule] default configuration page is as shown below:



Click the <New> button and the [Schedule] configuration dialog appears, as shown below:



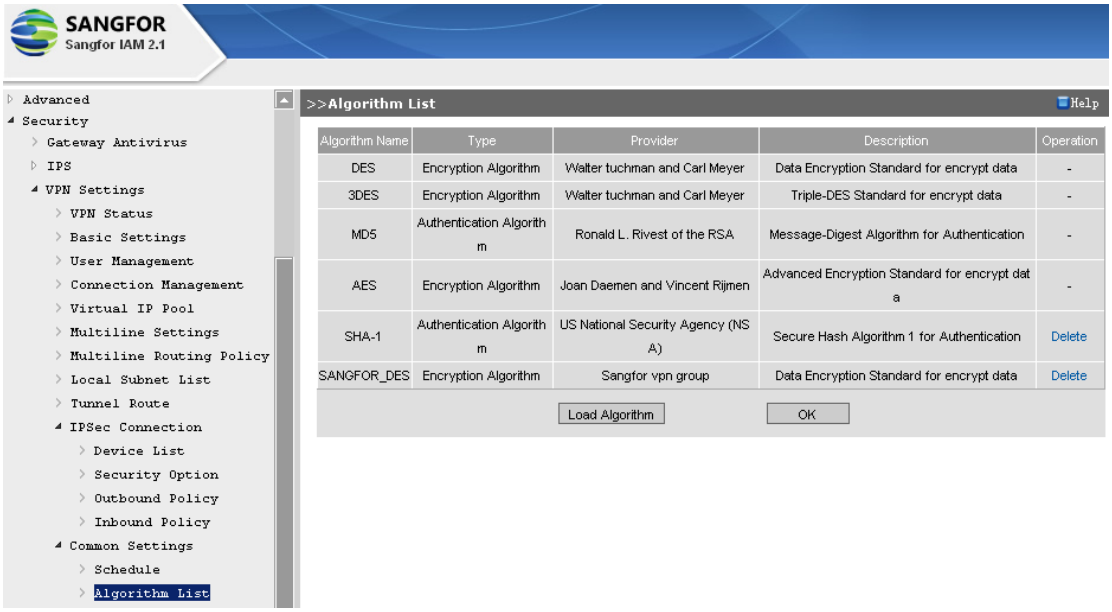
In this example, the "Office hours" is the enabled time period, which means, the rule will take effect during this period if it has referenced this schedule.

Having completed configuring this schedule, you have to click the <OK> button to save the settings.

13.3.11.2. Algorithm List

[Algorithm List] enables you to view and add the authentication algorithms and encryption algorithms that are supported by the SANGFOR IAM gateway device. These encryption algorithms will encrypt all the data transmitted over the established VPN network, guaranteeing security of these data.

The algorithm list is as shown below:



The SANGFOR IAM gateway device is integrated with some encryption algorithms and authentication algorithms such as MD5, SHA-1, DES, 3DES, AES, SANGFOR_DES. You can also add some other authentication or encryption algorithms. If necessary, please contact with SANGFOR.

13.3.12. Advanced

[Advanced] covers the configuration of [LAN Service], [VPN Interface], [LDAP Server] and [Radius Server].

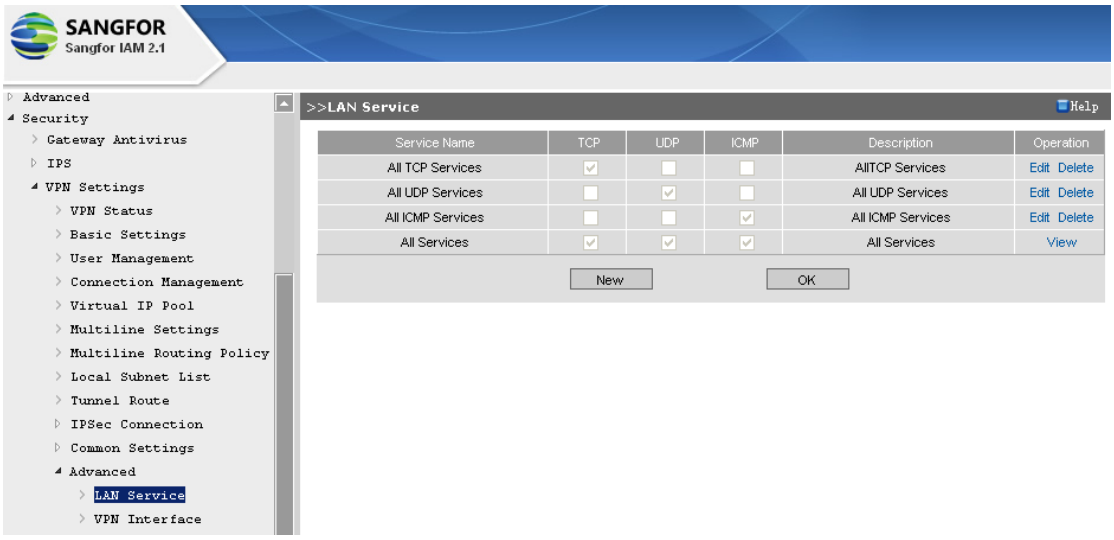
13.3.12.1. LAN Service

SANGFOR IAM gateway device enables you to specify the access privileges of the VPN users, or even to specify a branch VPN user or mobile VPN user (IP address) to access certain service(s) provided by a LAN computer; besides, it configures the service parameters of the inbound policy

used for connecting to a third-party device.

For example, to achieve the two requirements: a). only allow a user to access the WEB service provided by the headquarters WEB server (other services are unavailable for this user); b). allow an IP address of a branch VPN "branch1" to access the SQL server of the headquarters (other IP addresses of this branch are unable to access this server).

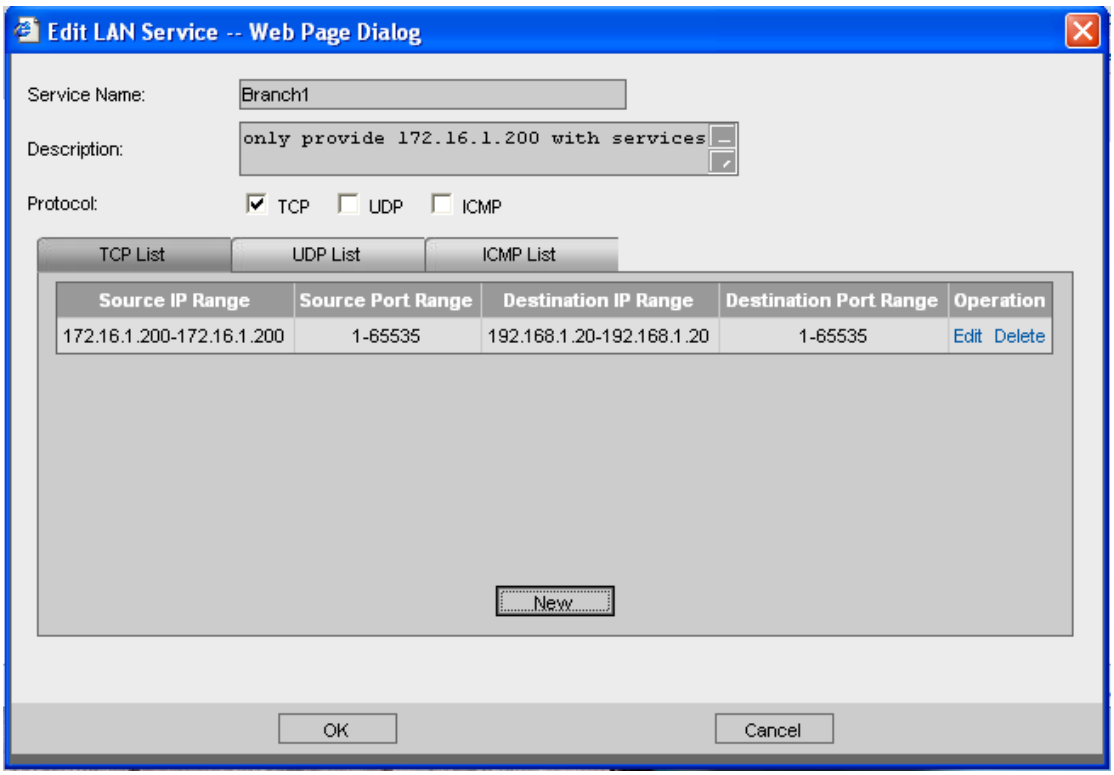
You have to configure the privilege of the relevant VPN user to certain service, so as to ensure the security of the VPN channels and achieve secure management.



Generally speaking, there are two steps to configure the privilege of the user to access LAN service: a). create LAN service; b). configure the privileges of the corresponding user.

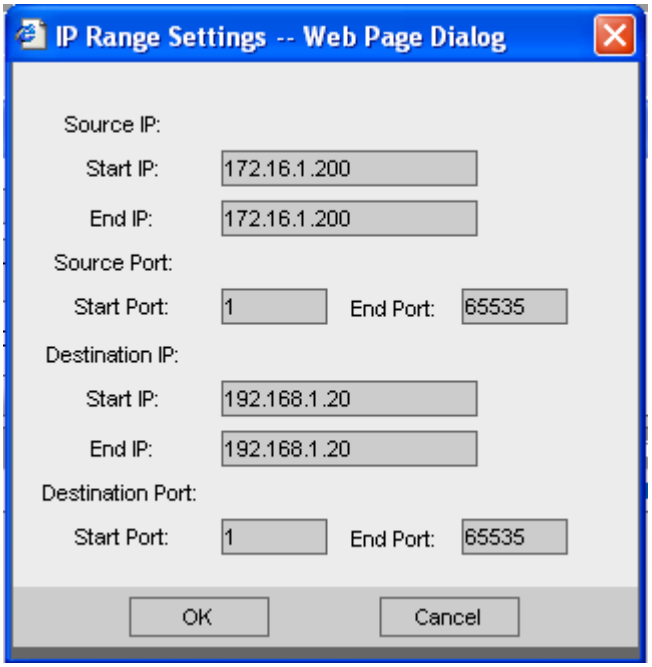
Take the following case as the example: allow an IP address (172.16.1.200) of branch1 to get access to the FTP server (192.168.1.20) of the headquarters; the requests for other service or the requests initiated by other IP addresses are denied. Detailed configuration steps are elaborated as below:

Under the default configuration page [LAN Service], click the <New> button to open the [Edit LAN Service] configuration dialog, as shown below:



Step 1: Type a name in the [Service Name] text box and check the protocol (in this example, it is FTP service, using TCP protocol).

Step 2: Click the <New> button to configure the IP ranges. The configuration dialog is as shown below:



[Source IP]: Fill in the source IP. In this example, it is the LAN IP address of the peer VPN, 172.16.1.200.

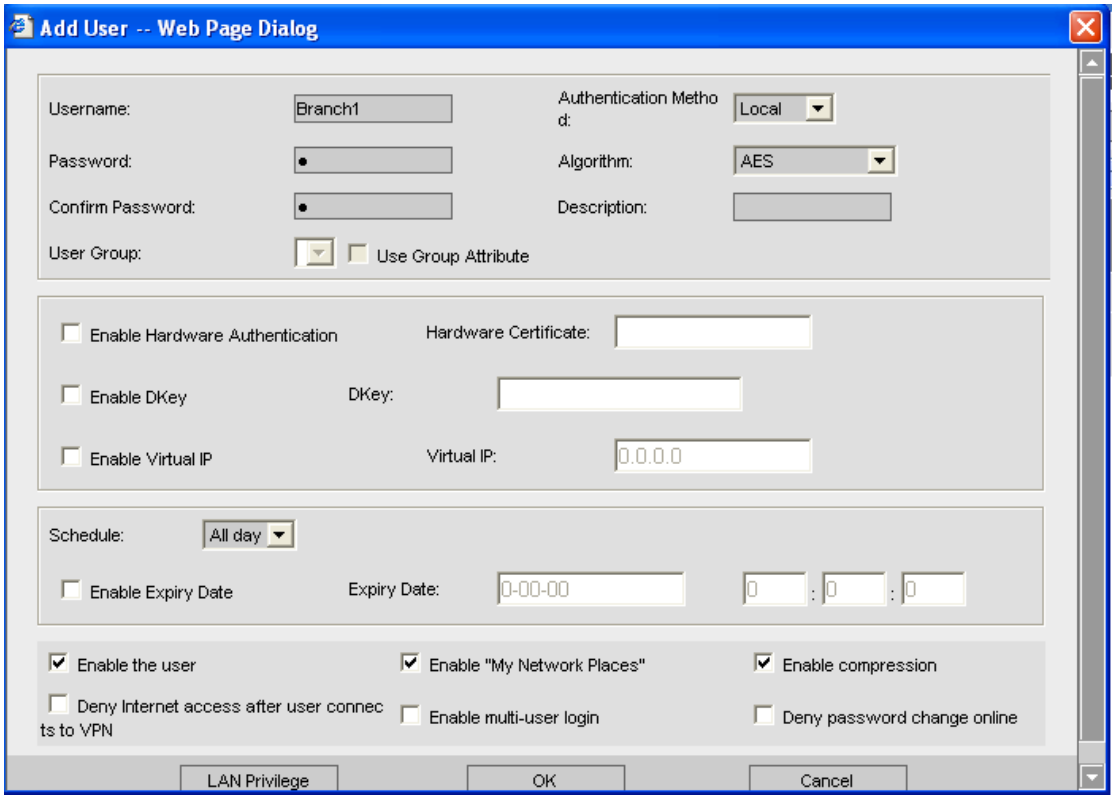
[Source port]: 1-65535.

[Destination IP]: Fill in the destination IP addresses. In this example, it is the FTP server IP of the headquarters, 192.168.1.20.

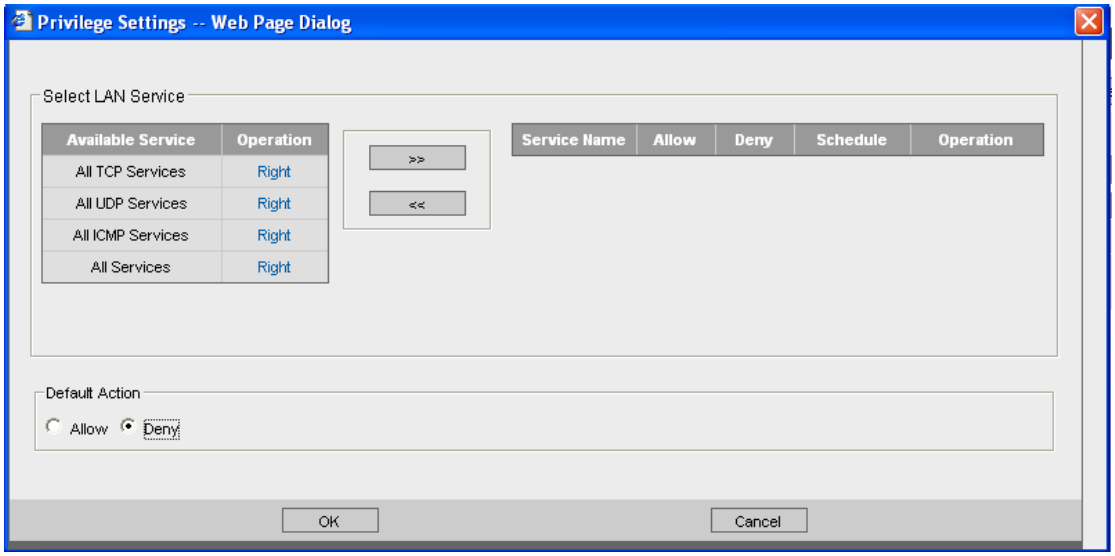
[Destination IP]: Port of FTP service is 20-21.

- The default configuration gives no limitation to the access privilege of VPN user.
- Here you are just "defining" the LAN services. After these configurations, you have to go to [Security] > [VPN Settings] > [User Management] to create an account (new user) and then configure the [LAN Privilege] to complete configuring the [LAN service].
- [LAN Service] can also be referred by the [IPSec Connection] > [Outbound Policy] and [Inbound Policy] configuration. For details, please refer to Section 13.4.10 IPSec Connection.

Step 3: Under the [User Management] page, select the user Branch1 and edit this user, as shown below:



Step 4: Click the <LAN Privilege> button and the [Privilege Settings] configuration dialog pops up, as shown below:



Step 5: Move the needed services to the service list (move from left to right) and check [Allow]. Select the [Deny] as the [Default Action].

Having completed configuring the above, you have to click the <OK> button to save the settings.

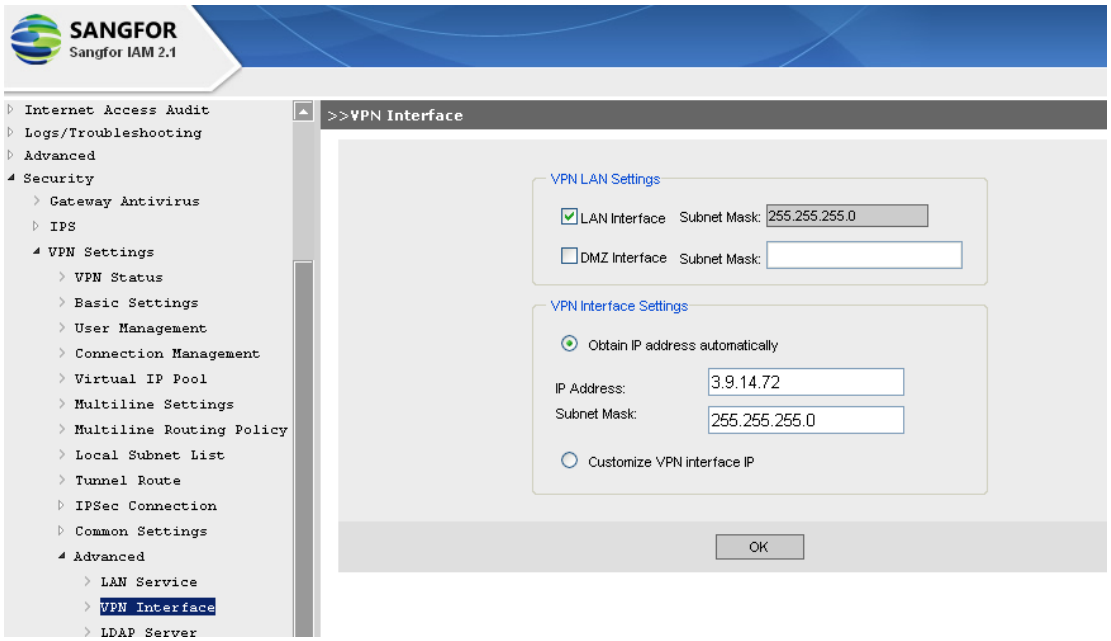
Till then, the configuring of [LAN Service] finishes; the branch1 user (172.16.1.200) can only access the FTP server (192.168.1.20), and the requests initiated by other IP address of that local area network will be denied.

These configurations also disable the access requests initiated by the other computers of the headquarters to access the Branch1. Because the [LAN Service] configurations will deny the response packet sent from other computers of the headquarters if the destination IP address is not 192.168.1.20 (IP address of the FTP server).

13.3.12.2. VPN Interface

[VPN Interface] configures the IP address of the virtual network adapter for the VPN service.

The configuration page is as shown below:

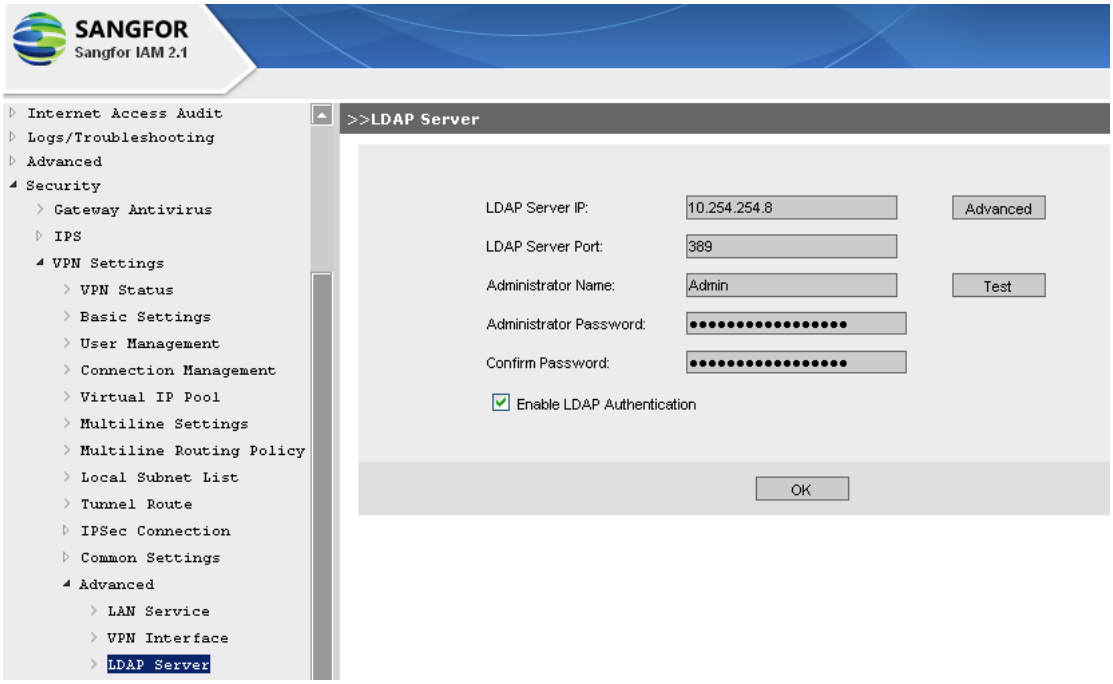


- By default, the [Obtain IP address automatically] option is checked. If IP conflict appears, you can also define the IP address.
- VPN interface is the virtual interface of the IAM gateway device. In reality, no such a physical interface is seen.

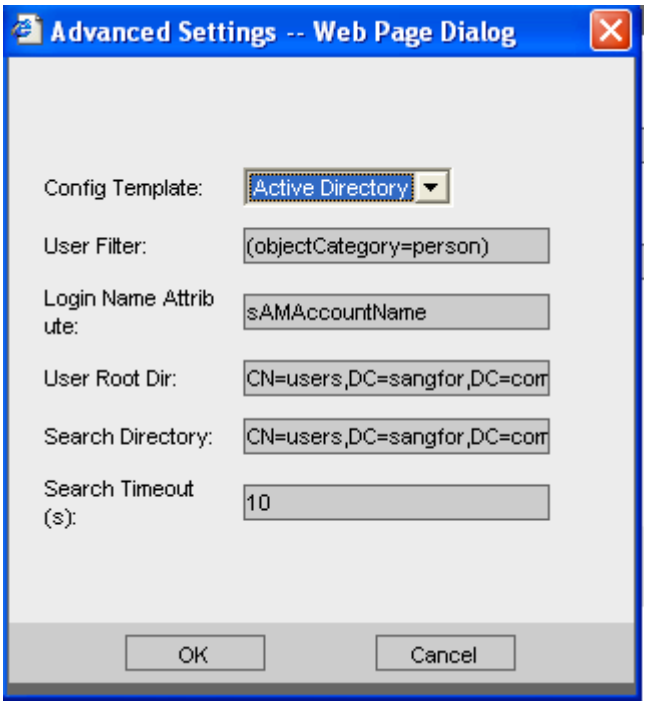
13.3.12.3. LDAP Server

The VPN service of SANGFOR IAM gateway supports LDAP authentication through a third party. If you need to have a third party to fulfill LDAP authentication, configure the [LDAP Server] (including configuration of [LDAP Server IP], [LDAP Server Port], [Administrator Name) by following the introduction and instructions below.

The [LDAP Server] configuration page is as shown below:



Having completed configuring the LDAP server (domain server), you can click the <Advanced> button to open the [Advanced Settings] dialog. The configuration dialog is as shown blow:



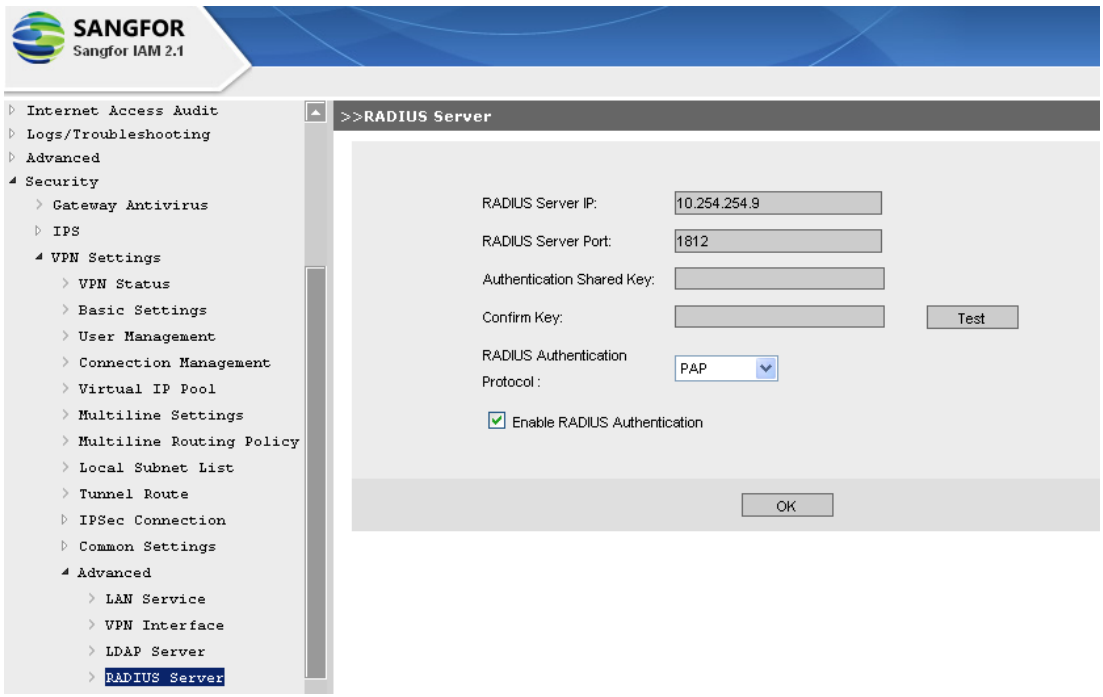
Configure these settings according to your case.

13.3.12.4. Radius Server

The VPN service of SANGFOR IAM gateway device supports RADIUS authentication through a

third party. If you want to have a third party fulfill the RADIUS authentication, correctly configure the [Radius Server] information (including [RADIUS Server IP], [RADIUS Server Port], [Authentication Shared Key] and [RADIUS Authentication Protocol]).

The configuration page is as shown below:



13.3.13. Generate Certificate

The HARDCA is one of the patents of SANGFOR. The device that applies this technology can use its certificate to get its identity authenticated among different VPN nodes. The certificate of a device is generated with some of the features of this device and is then encrypted. Due to the uniqueness of the device (hardware), the corresponding certificate is also unique and cannot be counterfeited. Through this way, requiring authentication with the features of the hardware, the IAM gateway device can ensure that only certain specified hardware device can get connected to a network, and therefore, eliminate the potential security hazards.

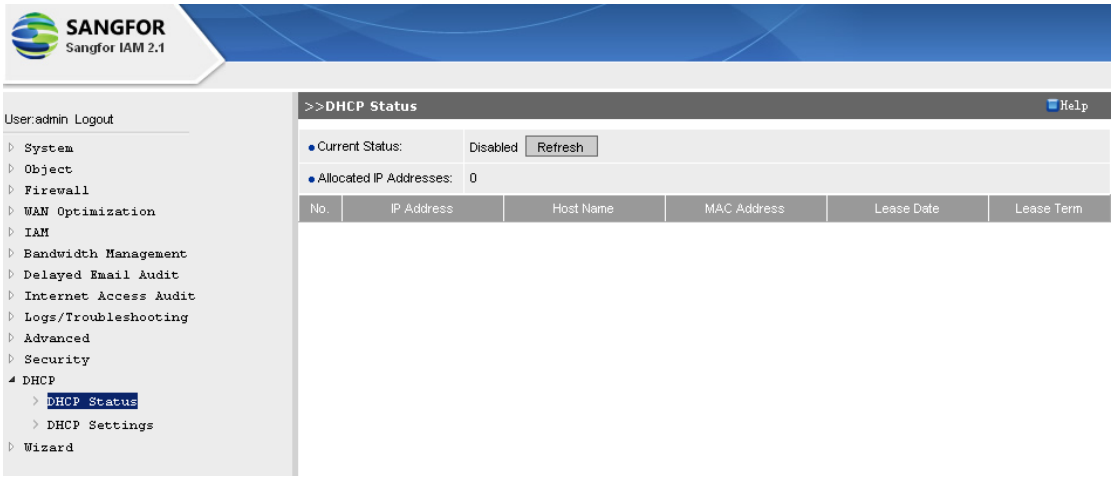
Click the <Generate> button and select a path to save the generated hardware certificate to the local computer.

Send this certificate to the administrator of the headquarters. Then, the administrator can check the [Enable Hardware Authentication] option, upload this hardware certificate and bind the user with this certificate while creating an account for this user.

Chapter 14 DHCP

14.1. DHCP Status

[DHCP Status] displays the running status of the DHCP and the IP addresses allocated to the LAN computers, details displayed are [Current status] of DHCP service, [Allocated IP Addresses], [Host Name] and [MAC Address].

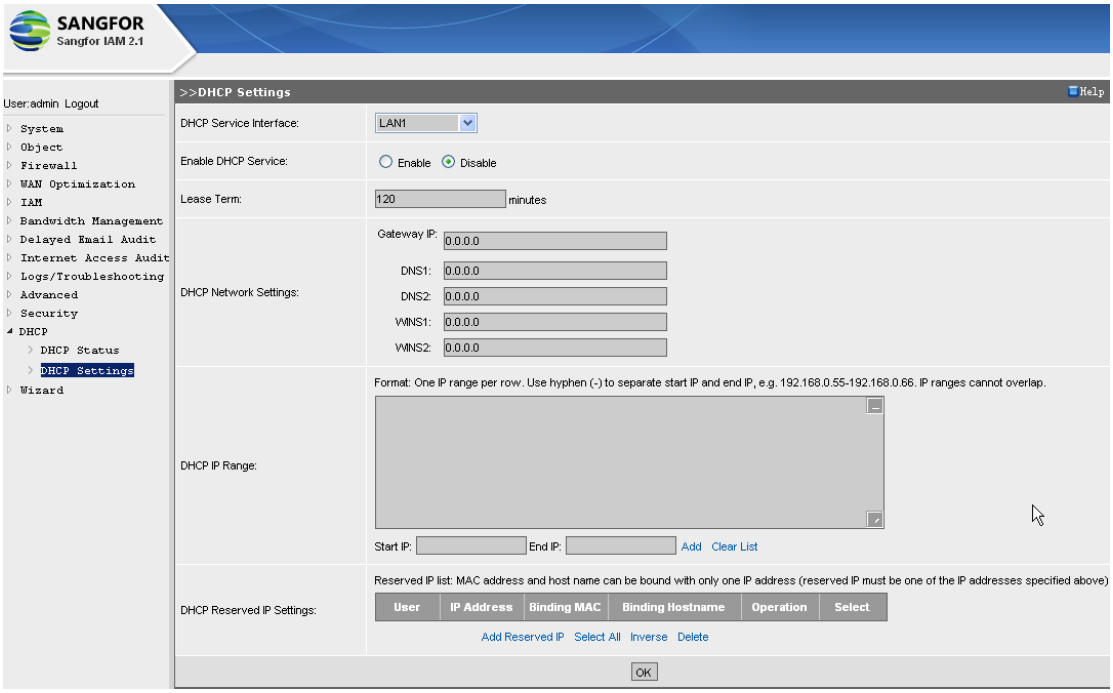


Click the <Refresh> button to refresh the status.

14.2. DHCP Settings

DHCP settings are detailed parameters of the DHCP service, including [DHCP Service Interface], [Gateway IP] of the allocated IP address, [Lease Term], [DNS], [WINS], [DHCP IP Range] and [DHCP Reserved IP Settings].

The configuration page is as shown below:



[DHCP Service Interface]: Select an interface for the DHCP service. You can use multiple network interfaces to fulfill DHCP services.

[Enable DHCP Service]: Select [Enable] to enable the DHCP (service) module.

[Lease Term]: Configures the expiry time of the IP address allocated by the DHCP.

[DHCP Network Settings]: Configures the [Gateway IP], [DNS] and [WINS] obtained by the DHCP client end. Generally, the [Gateway IP] is the corresponding [DHCP Service Interface] IP of the device. [DNS] is the DNS server IP provided by the local ISP, maximum two DNS supported; if neither of the DNS is configured, no DNS will be allocated to the client-end's computer. [WINS] is up to your specific application, being filled in or left blank.

[DHCP IP Ranges]: Type the start IP and end IP respectively in [Start IP] and [End IP] text boxes, and then click <Add> to add the IP range into the list.

[DHCP Reserved IP]: Configures the reserved IP address, and this reserved IP address will be allocated to the corresponding computer according the MAC address or hostname. Click <Add Reserved IP> and enter the [Username], [IP Address], [MAC Address] and [Hostname], among which,

[Username] is a user-defined name.

[IP Address] is a private network IP address that is to be reserved for this user.

The IP address reserved by the DHCP for this user can be bound according to the [MAC Address]

or [Hostname].

[Select] a user; type the [MAC Address] and [Hostname] and click <Obtain by IP> to get the corresponding parameter.

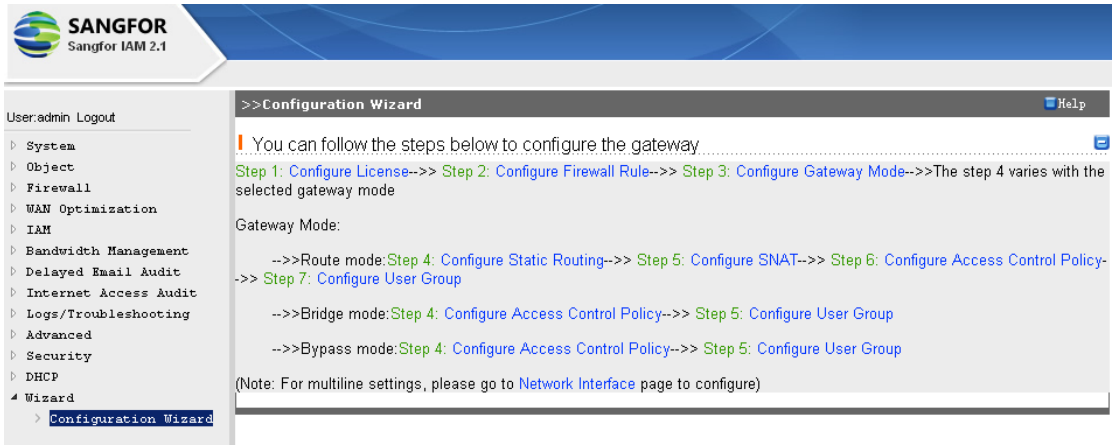
Finally, click the <OK> button to save the above settings.

- Be noted that the DHCP IP ranges configured here must not conflict with the static IP addresses of other working LAN computers.
- Generally, the IP address in the DHCP IP range list must not be the IP address whose last octet is 0 or 255, for these two addresses are network address and broadcast address of its network segment. For example, as to the 10.251.251.0 segment, the entered IP range can be 10.251.251.1-10.251.251.254.

Chapter 15 Wizard

[Configuration Wizard] introduces the flow and steps of the basic configurations, with link to configuring a specific module. Just click the item (in blue) to directly get into the corresponding configuration page.

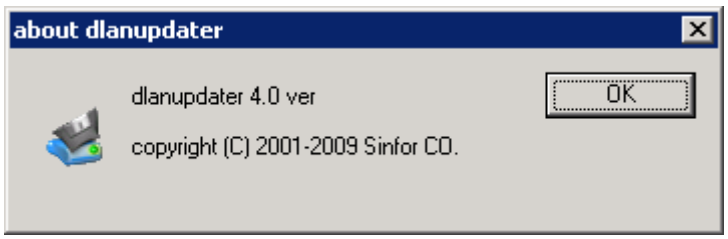
The page is as shown below:


SANGFOR
Sangfor IAM 2.1
User:admin Logout
System
Object
Firewall
WAN Optimization
IAM
Bandwidth Management
Delayed Email Audit
Internet Access Audit
Logs/Troubleshooting
Advanced
Security
DHCP
Wizard
Configuration Wizard
>>Configuration Wizard
Help
You can follow the steps below to configure the gateway
Step 1: Configure License-->> Step 2: Configure Firewall Rule-->> Step 3: Configure Gateway Mode-->>The step 4 varies with the selected gateway mode
Gateway Mode:
-->>Route mode:Step 4: Configure Static Routing-->> Step 5: Configure SNAT-->> Step 6: Configure Access Control Policy-->> Step 7: Configure User Group
-->>Bridge mode:Step 4: Configure Access Control Policy-->> Step 5: Configure User Group
-->>Bypass mode:Step 4: Configure Access Control Policy-->> Step 5: Configure User Group
(Note: For multiline settings, please go to Network Interface page to configure)

Appendix A: Gateway Client-Updater

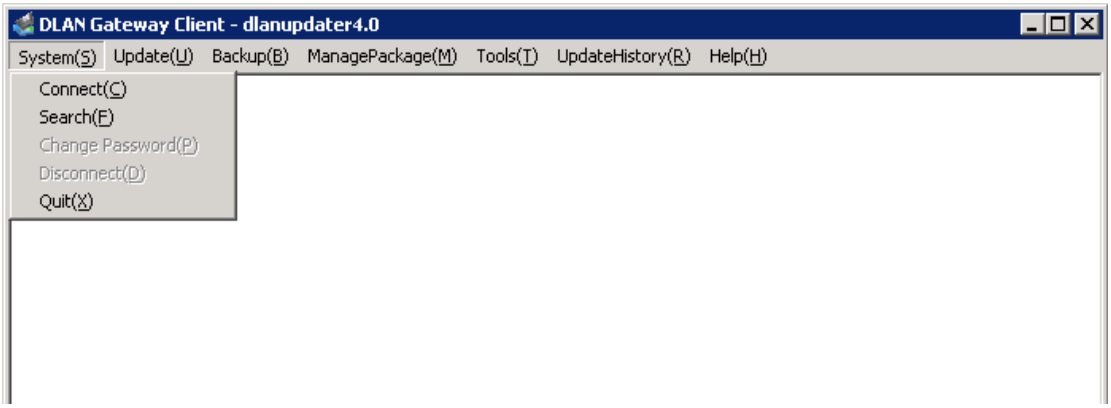
The gateway update and restoration system can be used to update the kernel version of SANGFOR IAM gateway device and backup configuration. When vital errors occur in the system, the IAM gateway device can be restored to the factory default configuration via the gateway restoration system. In addition, the gateway restoration system can be used to inspect the running state of the network interface and configuration of the routing, as well as to modify the working mode and MTU value of the network interface, etc.

As to the IAM gateway, gateway clients have to use **dlanupdater 4.0** DLAN Gateway Client. The configuration page is as shown below:



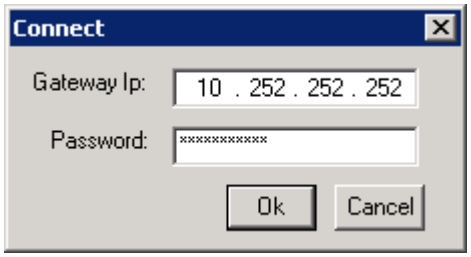
Menus included are [System], [Update], [Backup], [ManagePackage], [Tools], [Updatehistory] and [Help].

[System]: Submenus are [Connect], [Search], [Change password], [Disconnect] and [Quit].

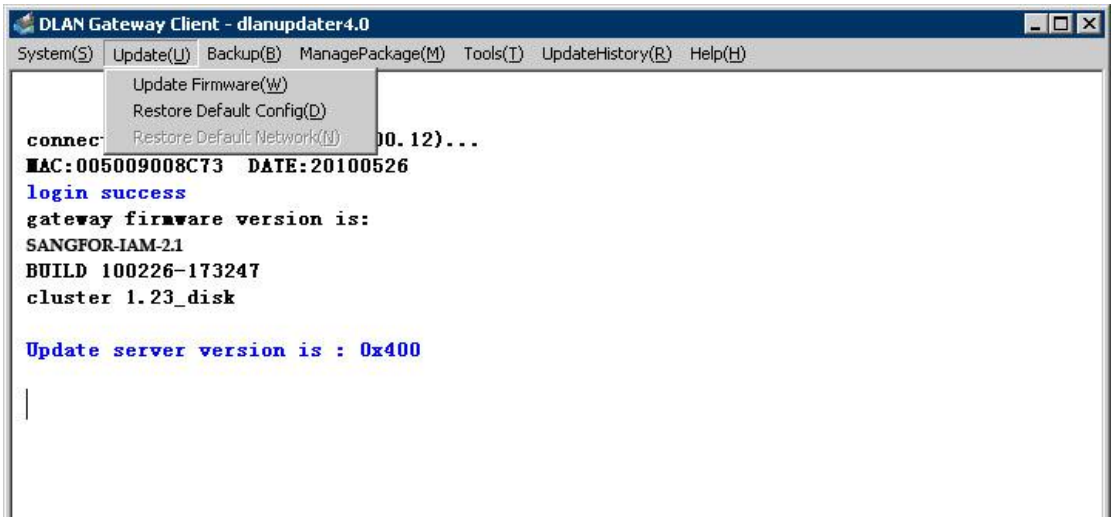


[Connect]: Directly enter the IP address of IAM hardware gateway device, and then type in the password to log in.

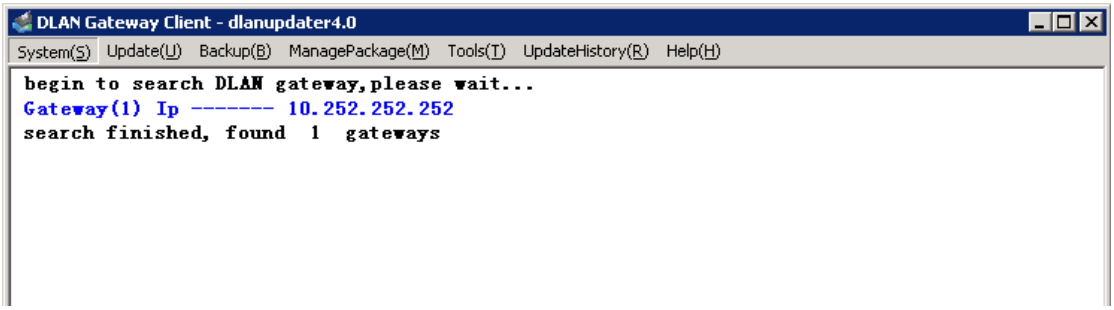
The default password is **dlanrecover**. The login page is as shown below.



After logging in successfully, it clews login success, as shown in the figure below:



[Search]: It will automatically search for the SANGFOR gateway devices, in the local area network (as long as there is no routing devices between the local computer and the IAM gateway device, and layer 2 broadcast can reach), even though the IAM gateway device is located in a different network segment (as long as there is no router or layer 3 switch between the local computer and the IAM gateway device). The search results are as shown in the following figure:


DLAN Gateway Client - dlanupdater4.0
System(S) Update(U) Backup(B) ManagePackage(M) Tools(T) UpdateHistory(R) Help(H)
begin to search DLAN gateway,please wait...
Gateway(1) Ip ------- 10.252.252.252
search finished, found 1 gateways

[Change password]: Modifies the login password of the gateway client-updater.

[Disconnect]: Cut the connection to the SANGFOR hardware gateway. If there is no operation for a certain time, the client terminal will be disconnected automatically.

[Update]: Submenus are [Update Firmware], [Restore Default Configuration], [Restore Default Network]. Please see the figure below:

[Update Firmware] and [Restore Default Configuration]: Both are only available after the user logging in IAM hardware gateway. The former ([Update Firmware]) is used for updating the kernel Firmware of IAM and the latter ([Restore Default Configuration]) for restoration of the default configuration. These operations will update the key document of the device, or will change serial number. Please DO NOT perform this operation at will. If update is needed, please contact the technicians of SANGFOR and follow the instructions.

[Restore Default Network]: This function is only available when the system is disconnected with the SANGFOR IAM hardware gateway. Conduct this function and the network configuration of the device will recover to defaults. This operation is realized with the command sent by the broadcast package, and will apply to all the SANGFOR hardware gateways deployed in the local area network (LAN).

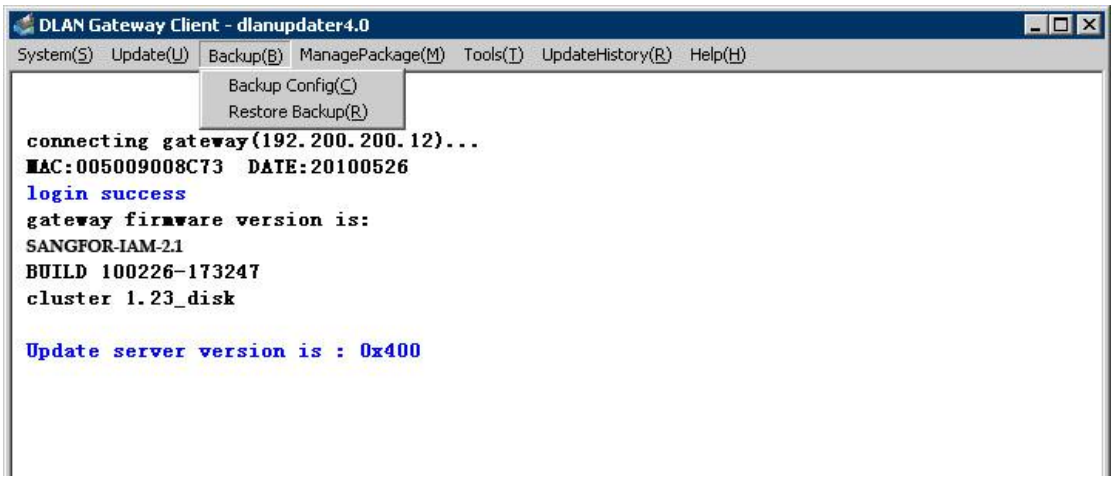
- Operation of [Restore Default Network] may result in hazardous outcome. Please DO NOT implement this function without second thought.
- IAM hardware gateway can only be updated from lower version to higher version; it does not allow skipping a version or degrading.
- Update is also a kind of risk. If update operation is not appropriate, the device may be damaged. Please DO NOT update the system by yourself at will. If necessary, please contact the technicians of SANGFOR for instructions.

Brief update procedures are:

Step1. Upload the corresponding update package to the Gateway Client-Updater.

Step2. Log in to the Gateway Client-Updater and implement update operations.

[Backup]: Submenus are [Backup Configuration], [Restore Backup]. Please refer to the page below:

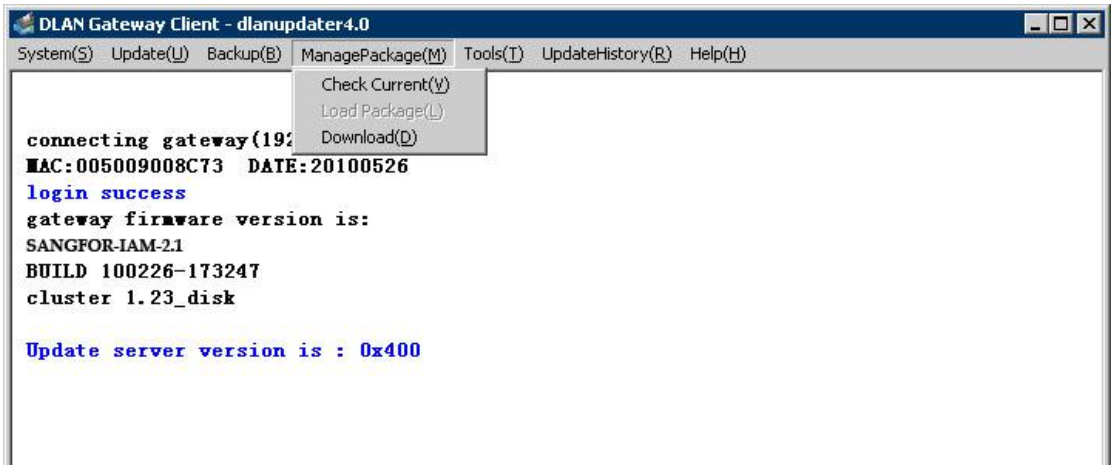


[Backup Config]: Backup all the configuration information of the IAM hardware gateway device.

[Restore Backup]: Restore all the backup configuration information to the IAM hardware gateway.

Operations of both are only applied to the same-model and same-version SANGFOR devices. Devices of different models and versions are inapplicable.

[Managepackage]: Submenus are [Check Current], [Load Package], [Download], as shown in the following figure:

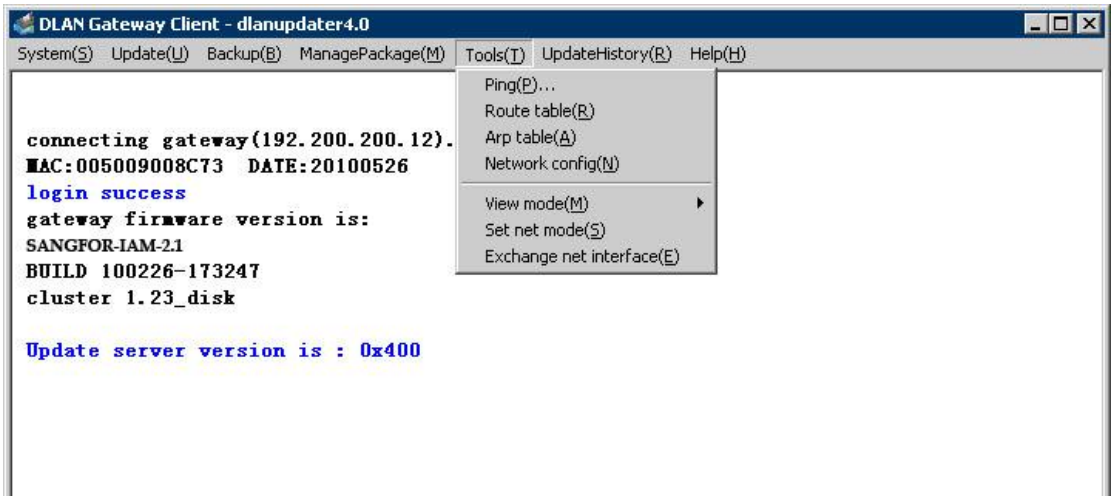


[Check Current]: View the information of the currently-loaded update package.

[Load Package]: Load the downloaded update package. Upload the update package. Only after implementation of the aforementioned procedures, can [Update]> [Update Firmware] be clicked.

[Download]: Please visit the SANGFOR official website *www.sangfor.com* to download the corresponding update package.

[Tools]: Submenus are [Ping], [Route Table], [ARP Table], [Network Config], [View Mode], [Set Net Mode], [Exchange Net Interface], as shown in the following figure:



[Ping]: Log in to the IAM gateway device, **ping** an external network on the device to check whether the IAM is connected to the external networks.

[Route Table]: View the route table of the IAM gateway device.

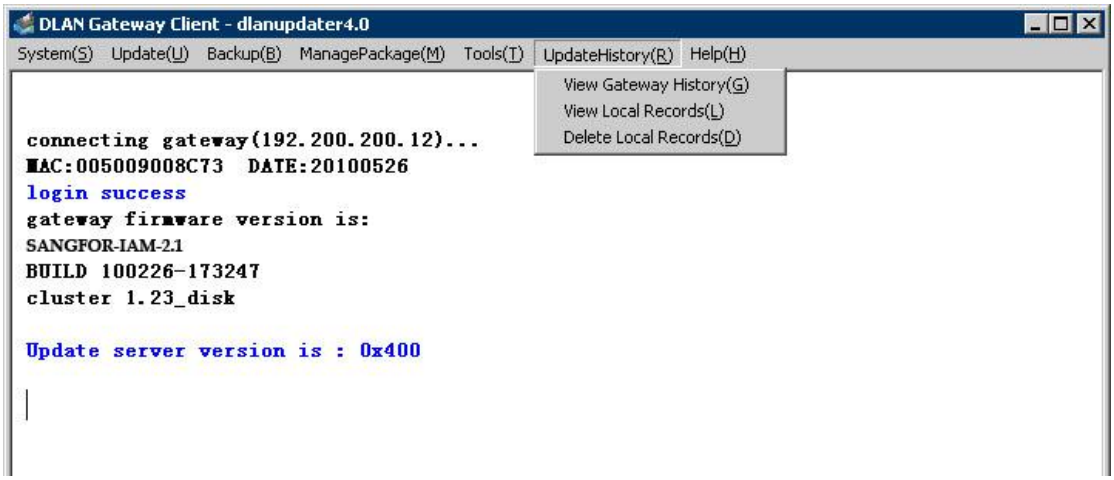
[ARP Table]: View the ARP table of the IAM gateway device.

[Network Config]: View the network configuration of the IAM gateway device, including information of interface IP, etc.

[View Mode]: View the mode the current network interface card (NIC) is working in.

[Set Net Mode]: Configure manually the working mode of NIC for the IAM gateway device, if the setting is not coherent to the actual network interface card mode.

[Update History]: Submenus are [View Gateway History], [View Local Records], [Delete Local Records], as shown in the following figure:



[View Gateway History]: View the update log of the IAM gateway device.

[View Local Records]: View the update log of the local Gateway Client-Updater.

[Delete Local Records]: Clear the update logs of the local Gateway Client-Updater.

Detailed Update Procedures:

a.) Download the update package to the local device.

b.) Start the Gateway Client-Updater and then load the downloaded update package (through [ManagePackage] > [Load Package]).

c.) Log in to the IAM gateway device through [System] > [Connect].

d.) Click [Update] > [Update Firmware], and the dlanupdater will prompt updating successfully, and then the IAM gateway device will reboot.

e.) If the default configurations need to be restored, log in to the device and click [Update] > [Restore Default Config].

To update the Firmware kernel of the SANGFOR gateway device, please DO follow the instructions given by the technicians of SANGFOR.

Appendix B: Acronyms And Abbreviations

AC	Alternating Current
AD	Active Directory
ARP	Address Resolution Protocol
BM	Bandwidth Management
CA	Certificate Authority
CPU	Central Processing Unit
DNAT	Destination Network Address Translation
DNS	Domain Name Server
DoS	Denial of Service Attack
HA	High Availability
HTTP	Hyper Test Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IM	Instant Message
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MTU	Maximum Transmission Unit
NIC	Network Interface Card
OS	Operating System
OSI	Open System Interconnect Reference Model
OU	Organization Unit
POP3	Post Office Protocol 3
SC	Secure Center
SMTP	Simple Message Transfer Protocol
SNAT	Source Network Address Translation
SSL	Secure Sockets Layer
SSO	Single Sign-On
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

UI	User Interface
URL	Uniform Resource Locator
VID	VLAN ID
VLAN	Virtual Local Area Network